

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



**Ministry
of Justice**

DATED 22 September 2025

(1) THE SECRETARY OF STATE FOR JUSTICE
and
(2) VODAFONE LIMITED

CONTRACT
relating to
provision of WAN Services
Contract reference: [REDACTED]

CORE TERMS

Core Terms	1 - 84

SCHEDULE 1 - DEFINITIONS

Schedule 1 - Definitions	85 - 164

SCHEDULE 2 - SERVICES DESCRIPTION

Schedule 2 - Services Description	165 - 172
Schedule 2 - Services Description Annex A (WAN Technical Requirements)	173 - 209
Schedule 2 - Services Description Annex B (WAN Service Management Requirements)	210 - 249
Schedule 2 - Services Description Annex C (WAN Transition Requirements)	250 - 262
Schedule 2 - Services Description Annex D (WAN Social Value Requirements)	263 - 268

SCHEDULE 3 - PERFORMANCE LEVELS

Schedule 3 - Performance Levels	269 - 310

SCHEDULE 4 - STANDARDS

Schedule 4 - Standards	311 - 328

SCHEDULE 5 - SECURITY MANAGEMENT

Schedule 5 - Security Management	329 - 383

SCHEDULE 6 - INSURANCE REQUIREMENTS

Schedule 6 - Insurance Requirements	384 - 390

SCHEDULE 7 - AUTHORITY RESPONSIBILITIES

Schedule 7 - Authority Responsibilities	391 - 398

SCHEDULE 8 - SUPPLIER SOLUTION

Schedule 8 - Supplier Solution	399 - 416
Schedule 8 - Supplier Solution - Annex A (Technical Solution)	417 - 478
Schedule 8 - Supplier Solution - Annex B (Service Management Solution)	479 - 536
Schedule 8 - Supplier Solution - Annex C (Transition Solution)	537 - 604
Schedule 8 - Supplier Solution - Annex D (Resource Profile)	605 - 641

SCHEDULE 9 - COMMERCIALLY SENSITIVE INFORMATION

Schedule 9 - Commercially Sensitive information 642 - 644

SCHEDULE 10 - NOTIFIED KEY SUBCONTRACTORS

Schedule 10 - Notified Key Subcontractors 645 - 646

SCHEDULE 11 - THIRD PARTY CONTRACTS

Schedule 11 - Third Party Contracts 647 - 656

SCHEDULE 12 - SOFTWARE

Schedule 12 - Software 657 - 667

SCHEDULE 13 - IMPLEMENTATION PLAN

Schedule 13 - Implementation Plan 668 - 716

SCHEDULE 14 - TESTING PROCEDURES

Schedule 14 - Testing Procedures 717 - 735

SCHEDULE 15 - CHARGES AND INVOICING

Schedule 15 - Charges and Invoicing 736 - 803

Schedule 15 - Charges and Invoicing - Annex H 804 - 821

SCHEDULE 16 - PAYMENTS ON TERMINATION

Schedule 16 - Payments on Termination 822 - 831

SCHEDULE 17 - BENCHMARKING

Schedule 17 - Benchmarking 832 - 847

SCHEDULE 18 - FINANCIAL DISTRESS

Schedule 18 - Financial Distress 848 - 868

SCHEDULE 19 - FINANCIAL REPORTS AND AUDIT RIGHTS

Schedule 19 - Financial Reports and Audit Rights 869 - 883

SCHEDULE 20 - ANTICIPATED SAVINGS

Schedule 20 - Anticipated Savings 884 - 885

SCHEDULE 21 - GOVERNANCE

Schedule 21 - Governance 886 - 916

SCHEDULE 22 - CHANGE CONTROL PROCEDURE

Schedule 22 - Change Control Procedure 917 - 945

SCHEDULE 23 - DISPUTE RESOLUTION PROCEDURE

Schedule 23 - Dispute Resolution Procedure 946 - 956

SCHEDULE 24 - REPORTS AND RECORDS PROVISION

Schedule 24 - Reports and Records Provision 957 - 985

SCHEDULE 25 - EXIT MANAGEMENT

Schedule 25 - Exit Management 986 - 1028

SCHEDULE 26 - SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING

Schedule 26 - Service Continuity Plan and Corporate Resolution Planning 1029 - 1049

SCHEDULE 27 - CONDUCT OF CLAIMS

Schedule 27 - Conduct of Claims 1050 - 1052

SCHEDULE 28 - STAFF TRANSFER

Schedule 28 - Staff Transfer 1053 - 1097

SCHEDULE 29 - KEY PERSONNEL

Schedule 29 - Key Personnel 1098 - 1103

SCHEDULE 30 - DEED OF GUARANTEE

Schedule 30 - Deed of Guarantee 1104 - 1114

SCHEDULE 31 - PROCESSING PERSONAL DATA

Schedule 31 - Processing Personal Data 1115 - 1142

SCHEDULE 32 - INTELLECTUAL PROPERTY RIGHTS

Schedule 32 - Intellectual Property Rights 1143 - 1153

SCHEDULE 33 - SERVICE RECIPIENTS

Schedule 33 - Service Recipients 1154 - 1158

SCHEDULE 34 - TRANSITIONAL SERVICES

Schedule 34 - Transitional Services 1159 - 1179

Annex 01 - TS Definitions 1180 - 1207

Annex 02 - Transitional Services Description 1208 - 1216

SCHEDULE 34 - TRANSITIONAL SERVICES (cont...)

Annex 02 Appendix A - TS Service Management Requirements	1217 - 1322
Annex 02 Appendix B - TS Technical Requirements	1323 - 1352
Annex 03 - TS Performance Levels	1353 - 1402
Annex 04 - TS Standards	1403 - 1414
Appendix 1 - TS Services Operations Manual to Annex 4 (TS Standards)	1415 - 1494
Annex 05 - TS Security Management	1495 - 1548
Annex 07 - Authority TS Responsibilities	1549 - 1550
Annex 08 - Supplier TS Solution	1551 - 1633
Annex 09 - TS Commercially Sensitive Information	1634 - 1637
Annex 10 - Notified TS Key Subcontractors	1638 - 1639
Annex 11 - TS Third Party Contracts	1640 - 1641
Annex 12 - TS Software	1642 - 1659
Annex 15 - TS Charges and Invoicing	1660 - 1687
Annex 16 - Payments on TS Termination	1688 - 1696
Annex 25 - TS Exit Management	1697 - 1705
Annex 29 - TS Key Personnel	1706 - 1707
Annex 32 - TS Intellectual Property Rights	1708 - 1719

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



**Ministry
of Justice**

DATED

22 September

2025

(1) THE SECRETARY OF STATE FOR JUSTICE

and

(2) VODAFONE LIMITED

CONTRACT

relating to

provision of WAN Services

Contract reference: [REDACTED]

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

CONTENTS

SECTION A – PRELIMINARIES	5
1 DEFINITIONS AND INTERPRETATION	5
2 DUE DILIGENCE	6
3 WARRANTIES	7
SECTION B – THE SERVICES	10
4 TERM	10
5 SERVICES	10
6 IMPLEMENTATION	17
7 PERFORMANCE INDICATORS	18
8 SERVICES IMPROVEMENT	20
9 EQUIPMENT AND MAINTENANCE	21
SECTION C – PAYMENT, TAXATION AND VALUE FOR MONEY PROVISIONS	24
10 FINANCIAL AND TAXATION MATTERS	24
SECTION D – CONTRACT GOVERNANCE	26
11 GOVERNANCE	26
12 RECORDS, REPORTS, AUDITS & OPEN BOOK DATA	26
13 CHANGE	26
SECTION E – SUPPLIER PERSONNEL AND SUPPLY CHAIN	28
14 SUPPLIER PERSONNEL	28
15 SUPPLY CHAIN RIGHTS AND PROTECTIONS	31
SECTION F – INTELLECTUAL PROPERTY, DATA AND CONFIDENTIALITY	40
16 INTELLECTUAL PROPERTY RIGHTS	40
17 IPRs INDEMNITY	40
18 AUTHORITY DATA AND SECURITY REQUIREMENTS	41
19 CONFIDENTIALITY	42
20 TRANSPARENCY AND FREEDOM OF INFORMATION	44
21 PROTECTION OF PERSONAL DATA	46
22 PUBLICITY AND BRANDING	53
SECTION G – LIABILITY, INDEMNITIES AND INSURANCE	54
23 LIMITATIONS ON LIABILITY	54
24 INSURANCE	57
SECTION H – REMEDIES AND RELIEF	58
25 RECTIFICATION PLAN PROCESS	58
26 DELAY PAYMENTS	60
27 REMEDIAL ADVISER	60
28 STEP-IN RIGHTS	62
29 AUTHORITY CAUSE	64
30 FORCE MAJEURE	66
SECTION I – TERMINATION AND EXIT MANAGEMENT	69
31 TERMINATION RIGHTS	69
32 CONSEQUENCES OF EXPIRY OR TERMINATION	70
SECTION J – MISCELLANEOUS AND GOVERNING LAW	74
33 COMPLIANCE	74
34 ASSIGNMENT AND NOVATION	78

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

35 WAIVER AND CUMULATIVE REMEDIES.....78

36 RELATIONSHIP OF THE PARTIES 79

37 PREVENTION OF FRAUD AND BRIBERY 79

38 SEVERANCE 80

39 FURTHER ASSURANCES 80

40 ENTIRE AGREEMENT 81

41 THIRD PARTY RIGHTS 81

42 NOTICES 81

43 DISPUTES 83

44 GOVERNING LAW AND JURISDICTION 83

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SCHEDULES

1. Definitions
2. Services Description
3. Performance Levels
4. Standards
5. Security Management
6. Insurance Requirements
7. Authority Responsibilities
8. Supplier Solution
9. Commercially Sensitive Information
10. Notified Key Sub-contractors
11. Third Party Contracts
12. Software
13. Implementation Plan
14. Testing Procedures
15. Charges and Invoicing
16. Payments on Termination
17. Benchmarking
18. Financial Distress
19. Financial Reports and Audit Rights
20. Anticipated Savings
21. Governance
22. Change Control Procedure, Service Requests and Projects
23. Dispute Resolution Procedure
24. Reports and Records Provisions
25. Exit Management
26. Service Continuity Plan and Corporate Resolution Planning
27. Conduct of Claims
28. Staff Transfer
29. Key Personnel
30. Guarantee
31. Processing Personal Data
32. Intellectual Property Rights
33. Service Recipients
34. Transitional Services

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

THIS CONTRACT is made on 22 September 2025

BETWEEN:

- (1) **THE SECRETARY OF STATE FOR JUSTICE acting as part of the Crown** of Ministry of Justice, Commercial and Contract Directorate, Zone 3.19, 3rd Floor, 10 South Colonnade, Canary Wharf E14 4PU (the “**Authority**”); and
- (2) **VODAFONE LIMITED** a company registered in England and Wales under company number 1471587 whose registered office is at Vodafone House, The Connection, Newbury, Berkshire RG14 2FN (the “**Supplier**”)

(each a “**Party**” and together the “**Parties**”).

INTRODUCTION

- (A) The Authority is responsible for the courts, prisons, probation services and attendance centres which form part of the justice system in England and Wales and wishes to procure the provision of wide area network (WAN) services.
- (B) On 25 May 2023 the Authority advertised on Find a Tender (reference 2023/S 000-014987), inviting prospective suppliers to submit proposals for the WAN Services which form part of the Authority’s ‘Evolve’ portfolio of procurements for ICT services.
- (C) The Supplier is a leading provider of telecommunication services and has experience in Wide Area Networks.
- (D) On the basis of the Supplier’s response to the advertisement and a subsequent tender process, the Authority selected the Supplier as its preferred supplier.
- (E) The Parties have agreed to contract with each other in accordance with the terms and conditions set out below.

IT IS AGREED as follows:

SECTION A – PRELIMINARIES

1 DEFINITIONS AND INTERPRETATION

- 1.1 In this Contract, unless otherwise provided or the context otherwise requires, capitalised expressions shall have the meanings set out in Schedule 1 (Definitions) or the relevant Schedule in which that capitalised expression appears.
- 1.2 Interpretation is as set out in Schedule 1 (Definitions).
- 1.3 If there is any conflict between the Clauses and the Schedules and/or any Annexes to the Schedules, the conflict shall be resolved in accordance with the following order of precedence:
 - (a) the Clauses and Schedule 1 (Definitions), unless the conflict relates to the provision of the Transitional Services, in which case Schedule

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

34 (Transitional Services) shall take precedence over the Clauses and the other Schedules and any conflict between the Paragraphs, Clauses, Schedules and Annexes within Schedule 34 shall be resolved in accordance with Paragraph 1.2 of Schedule 34 (Transitional Services);

- (b) Schedules 2 (Services Description) and 3 (Performance Levels) and their Annexes;
- (c) any other Schedules and their Annexes (other than Schedule 8 (Supplier Solution) and its Annexes); and
- (d) Schedule 8 (Supplier Solution) and its Annexes (if any) unless any part of the Supplier Solution offers a better commercial position for the Authority (as decided by the Authority, in its absolute discretion), in which case that part of the Supplier Solution will take precedence over the documents above.

1.4 The Schedules and their Annexes form part of this Contract.

1.5 In entering into this Contract the Authority is acting as part of the Crown.

2 DUE DILIGENCE

2.1 The Supplier acknowledges that, subject to the Allowable Assumptions:

- (a) the Authority has delivered or made available to the Supplier all of the information and documents that the Supplier considers necessary or relevant for the performance of its obligations under this Contract;
- (b) it has made its own enquiries to satisfy itself as to the accuracy and adequacy of the Due Diligence Information;
- (c) it has satisfied itself (whether by inspection or having raised all relevant due diligence questions with the Authority before the Effective Date) of all relevant details relating to:
 - (i) the Authority Requirements;
 - (ii) the suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Effective Date) future Operating Environment;
 - (iii) the operating processes and procedures and the working methods of the Authority;
 - (iv) the ownership, functionality, capacity, condition and suitability for use in the Services of the Authority Assets; and
 - (v) the existing contracts (including any licences, support, maintenance and other agreements relating to the Operating Environment) referred to in the Due Diligence Information which may be novated to, assigned to or managed by the

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Supplier under this Contract and/or which the Supplier will require the benefit of for the provision of the Services; and

- (d) it has advised the Authority in writing of:
- (i) each aspect, if any, of the Operating Environment that is not suitable for the provision of the Services;
 - (ii) the actions needed to remedy each such unsuitable aspect; and
 - (iii) a timetable for and, to the extent that such costs are to be payable to the Supplier, the costs of those actions,
- and such actions, timetable and costs are fully reflected in this Contract, including the Services Description and/or Authority Responsibilities as applicable.

2.2 The Supplier shall not be excused from the performance of any of its obligations under this Contract on the grounds of, nor, subject to Clause 2.3, shall the Supplier be entitled to recover any additional costs or charges, arising as a result of:

- (a) any unsuitable aspects of the Operating Environment;
- (b) any misinterpretation of the Authority Requirements; and/or
- (c) any failure by the Supplier to satisfy itself as to the accuracy and/or adequacy of the Due Diligence Information.

2.3 The Parties shall comply with the provisions of Paragraph 6 of Part C of Schedule 15 (*Charges and Invoicing*) in relation to the verification of any Allowable Assumptions.

3 WARRANTIES

3.1 The Authority represents and warrants that:

- (a) it has full capacity and authority to enter into and to perform this Contract;
- (b) this Contract is entered into by its duly authorised representative;
- (c) there are no actions, suits or proceedings or regulatory investigations before any court or administrative body or arbitration tribunal pending or, to its knowledge, threatened against it that might affect its ability to perform its obligations under this Contract; and
- (d) its obligations under this Contract constitute its legal, valid and binding obligations, enforceable in accordance with their respective terms subject to applicable bankruptcy, reorganisation, insolvency, moratorium or similar Laws affecting creditors' rights generally and subject, as to enforceability, to equitable principles of general

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

application (regardless of whether enforcement is sought in a proceeding in equity or law).

3.2 The Supplier represents and warrants that:

- (a) it is validly incorporated, organised and subsisting in accordance with the Laws of its place of incorporation;
- (b) it has full capacity and authority to enter into and to perform this Contract;
- (c) this Contract is entered into by its duly authorised representative;
- (d) it has all necessary consents and regulatory approvals to enter into this Contract;
- (e) it has notified the Authority in writing of any actions, suits or proceedings or regulatory investigations before any court or administrative body or arbitration tribunal pending or, to its knowledge, any threatened against it or any of its Affiliates that might affect its ability to perform its obligations under this Contract;
- (f) its execution, delivery and performance of its obligations under this Contract will not constitute a breach of any Law or obligation applicable to it and will not cause or result in a default under any agreement by which it is bound;
- (g) its obligations under this Contract constitute its legal, valid and binding obligations, enforceable in accordance with their respective terms subject to applicable bankruptcy, reorganisation, insolvency, moratorium or similar Laws affecting creditors' rights generally and subject, as to enforceability, to equitable principles of general application (regardless of whether enforcement is sought in a proceeding in equity or law);
- (h) all written statements and representations in any written submissions made by the Supplier as part of the procurement process, including without limitation its response to the selection questionnaire and ITT (if applicable), its tender and any other documents submitted remain true and accurate except to the extent that such statements and representations have been superseded or varied by this Contract or to the extent that the Supplier has otherwise disclosed to the Authority in writing prior to the date of this Contract;
- (i) it has notified the Authority in writing of any Occasions of Tax Non-Compliance and any litigation in which it is involved that is in connection with any Occasion of Tax Non-Compliance;
- (j) it has all necessary rights in and to the Licensed Software, the Third Party IPRs, the Supplier Background IPRs and any other materials made available by the Supplier (and/or any Sub-contractor) to the Authority which are necessary for the performance of the Supplier's

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- obligations under this Contract and/or the receipt of the Services by the Authority;
- (k) the Contract Inception Report is a true and accurate reflection of the Costs and Supplier Profit Margin forecast by the Supplier and the Supplier does not have any other internal financial model in relation to the Services inconsistent with the Financial Model;
 - (l) it is not subject to any contractual obligation, compliance with which is likely to have a material adverse effect on its ability to perform its obligations under this Contract;
 - (m) no proceedings or other steps have been taken and not discharged (nor, to the best of its knowledge, are threatened) for the winding up of the Supplier or for its dissolution or for the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Supplier's assets or revenue; and
 - (n) within the previous 12 months, no Financial Distress Events have occurred or are subsisting (or any events that would be deemed to be Financial Distress Events under this Contract had this Contract been in force) and there are currently no matters that it is aware of that could cause a Financial Distress Event to occur or subsist.
- 3.3 The representations and warranties set out in Clause 3.2 shall be deemed to be repeated by the Supplier on the Effective Date (if later than the date of signature of this Contract) by reference to the facts then existing.
- 3.4 Each of the representations and warranties set out in Clauses 3.1 and 3.2 shall be construed as a separate representation and warranty and shall not be limited or restricted by reference to, or inference from, the terms of any other representation, warranty or any other undertaking in this Contract.
- 3.5 If at any time a Party becomes aware that a representation or warranty given by it under Clause 3.1 or 3.2 has been breached, is untrue or is misleading, it shall immediately notify the other Party of the relevant occurrence in sufficient detail to enable the other Party to make an accurate assessment of the situation.
- 3.6 For the avoidance of doubt, the fact that any provision within this Contract is expressed as a warranty shall not preclude any right of termination which the Authority may have in respect of breach of that provision by the Supplier.
- 3.7 Except as expressly stated in this Contract, all warranties and conditions whether express or implied by statute, common law or otherwise are hereby excluded to the extent permitted by Law.
- 3.8 The Supplier indemnifies the Authority against wilful misconduct of the Supplier, Subcontractor and Supplier Personnel that impacts the Contract.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SECTION B – THE SERVICES**4 TERM**

4.1 This Contract shall:

- (a) come into force on the Effective Date; and
- (b) unless terminated at an earlier date by operation of Law or in accordance with Clause 31 (*Termination Rights*), terminate:
 - (i) at the end of the Initial Term; or
 - (ii) if the Authority elects to extend the Term beyond the Initial Term by giving the Supplier at least sixty (60) Working Days' notice before the end of the Initial Term, at the end of the First Extension Period; or
 - (iii) if the Authority elects to extend the Term beyond the First Extension Period or the Second Extension Period by giving the Supplier at least twenty (20) Working Days' notice before the end of the First Extension Period or the Second Extension Period (as applicable), at the end of the Second Extension Period or the Third Extension Period (whichever is relevant). For the avoidance of doubt, the First Extension Period and any Second Extension Period or Third Extension Period should each be for one (1) year.

5 SERVICES**Standard of Services**

5.1 The Supplier shall provide:

- (a) the Transitional Services from (and including) the Transitional Services Commencement Date; and
- (b) the Implementation Services from (and including) the Implementation Services Commencement Date; and
- (c) the Operational Services in each case from (and including) the relevant Operational Service Commencement Date,

in each case for the benefit of the Authority and the Service Recipients.

5.2 The Supplier shall ensure that:

- (a) the Services:
 - (i) comply in all respects with the Services Description; and
 - (ii) are supplied in accordance with the Supplier Solution and the provisions of this Contract; and

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

(b) where:

- (i) the Operational Services to be provided from any Operational Service Commencement Date are similar to services that the Authority was receiving immediately prior to the Effective Date (such similar services being "**Preceding Services**"); and
- (ii) the standard and level of service received by the Authority in respect of any of the Preceding Services in a 12 month period ending between four months prior to or on the Effective Date (a) have been disclosed to the Supplier in the Due Diligence Information or (b) are known or ought reasonably to be known by the Supplier in its capacity as the incumbent supplier of such services to the Authority (such preceding services being "**Relevant Preceding Services**"),

the Operational Services to be provided from the relevant Operational Service Commencement Date that are similar to the Relevant Preceding Services are in each case provided to a standard and level of service which is at least as good as the standard and level of service received by the Authority in respect of the Relevant Preceding Services in the 12 month period for which information has been disclosed in accordance with Clause 5.2(b)(ii).

5.3 The Supplier shall:

- (a) perform its obligations under this Contract, including in relation to the supply of the Services and any Goods in accordance with:
 - (i) all applicable Law;
 - (ii) Good Industry Practice;
 - (iii) the Standards and the Processes;
 - (iv) the Baseline Security Requirements;
 - (v) the Quality Plans;
 - (vi) the Authority IT Strategy; and
 - (vii) the Supplier's own established procedures and practices to the extent the same do not conflict with the requirements of Clauses 5.3(a)(i) to 5.3(a)(vi); and
- (b) indemnify the Authority against any costs resulting from any breach by the Supplier of any applicable Law relating to the Contract; and
- (c) deliver the Services using efficient business processes and ways of working having regard to the Authority's obligation to ensure value for money.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 5.4 In the event that the Supplier becomes aware of any inconsistency between the requirements of Clauses 5.3(a)(i) to 5.3(a)(vi), the Supplier shall immediately notify the Authority Representative in writing of such inconsistency and the Authority Representative shall, as soon as practicable, notify the Supplier which requirement the Supplier shall comply with.

Supplier covenants

- 5.5 The Supplier shall:

- (a) at all times allocate sufficient resources with the appropriate technical expertise to supply the Deliverables and to provide the Services in accordance with this Contract;
- (b) save to the extent that obtaining and maintaining the same are Authority Responsibilities and subject to Clause 13 (*Change*), obtain, and maintain throughout the duration of this Contract, all the consents, wayleaves, approvals, licences and permissions (statutory, regulatory contractual or otherwise) it may require and which are necessary for the provision of the Services;
- (c) ensure that:
 - (i) it shall continue to have all necessary rights in and to the Licensed Software, the Third Party IPRs, the Supplier Background IPRs and any other materials made available by the Supplier (and/or any Sub-contractor) to the Authority which are necessary for the performance of the Supplier's obligations under this Contract and/or the receipt of the Services by the Authority;
 - (ii) the release of any new Software or upgrade to any Software complies with the interface requirements in the Services Description and (except in relation to new Software or upgrades which are released to address Malicious Software or to comply with the requirements of Schedule 5 (*Security Management*)) shall notify the Authority 3 months before the release of any new Software or Upgrade;
 - (iii) all Software including Upgrades, Updates and New Releases used by or on behalf of the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;
 - (iv) any products or services recommended or otherwise specified by the Supplier for use by the Authority in conjunction with the Deliverables and/or the Services shall enable the Deliverables and/or Services to meet the Authority Requirements; and

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (v) the Supplier System and Assets used in the performance of the Services will be free of all encumbrances (except as agreed in writing with the Authority);
- (d) minimise any disruption to the Services, the IT Environment and/or the Authority's operations when carrying out its obligations under this Contract;
- (e) ensure that any Documentation and training provided by the Supplier to the Authority are comprehensive, accurate and prepared in accordance with Good Industry Practice;
- (f) co-operate with any Other Supplier notified to the Supplier by the Authority from time to time by providing:
 - (i) reasonable information (including any Documentation);
 - (ii) advice; and
 - (iii) reasonable assistance,

in connection with the Services to any such Other Supplier to enable such Other Supplier to create and maintain technical or organisational interfaces with the Services and, on the expiry or termination of this Contract for any reason, to enable the timely transition of the Services (or any of them) to the Authority and/or to any Replacement Supplier in accordance with the following collaborative working principles:

- (A) proactively leading on, mitigating and contributing to the resolution of problems or issues irrespective of its contractual obligations, acting in accordance with the principle of "fix first, settle later";
- (B) being open, transparent and responsive in sharing relevant and accurate information with such Other Suppliers;
- (C) where reasonable, adopting common working practices, terminology, standards and technology and a collaborative approach to service development and resourcing with such Other Suppliers;
- (D) providing reasonable cooperation, support, information and assistance to such Other Suppliers in a proactive, transparent and open way and in a spirit of trust and mutual confidence; and
- (E) identifying, implementing and capitalising on opportunities to improve Deliverables and deliver better solutions and performance throughout the relationship lifecycle;

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (g) to the extent it is legally able to do so, hold on trust for the sole benefit of the Authority, all warranties and indemnities provided by third parties or any Sub-contractor in respect of any Deliverables and/or the Services and, where any such warranties are held on trust, at its cost enforce such warranties in accordance with any reasonable directions that the Authority may notify from time to time to the Supplier;
 - (h) unless it is unable to do so, assign to the Authority on the Authority's written request and at the cost of the Supplier any such warranties and/or indemnities as are referred to in Clause 5.5(g);
 - (i) provide the Authority with such assistance as the Authority may reasonably require during the Term in respect of the supply of the Services;
 - (j) gather, collate and provide such information and co-operation as the Authority may reasonably request for the purposes of ascertaining the Supplier's compliance with its obligations under this Contract;
 - (k) notify the Authority in writing as soon as reasonably possible and in any event within 1 month of any change of Control taking place;
 - (l) notify the Authority in writing within 10 Working Days of their occurrence, of any actions, suits or proceedings or regulatory investigations before any court or administrative body or arbitration tribunal pending or, to its knowledge, threatened against it that might affect its ability to perform its obligations under this Contract;
 - (m) ensure that neither it, nor any of its Affiliates, embarrasses the Authority or otherwise brings the Authority into disrepute by engaging in any act or omission in relation to this Contract which is reasonably likely to diminish the trust that the public places in the Authority; and
 - (n) manage closure or termination of Services and end of life of Goods to take account of the Authority's disposal requirements, including recycling and scope for re-use, and all applicable Standards.
- 5.6 An obligation on the Supplier to do, or to refrain from doing, any act or thing shall include an obligation upon the Supplier to procure that all Sub-contractors and Supplier Personnel also do, or refrain from doing, such act or thing.
- 5.7 Without prejudice to Clauses 17.2 and 17.3 (*IPRs Indemnity*) and any other rights and remedies of the Authority howsoever arising, the Supplier shall:
- (a) remedy any breach of its obligations in Clauses 5.5(b) to 5.5(d) inclusive within 3 Working Days of becoming aware of the breach or being notified of the breach by the Authority where practicable or within such other time period as may be agreed with the Authority (taking into account the nature of the breach that has occurred);

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) remedy any breach of its obligations in Clause 5.5(a) and Clauses 5.5(e) to 5.5(j) inclusive within 20 Working Days of becoming aware of the breach or being notified of the breach by the Authority; and
- (c) meet all the costs of, and incidental to, the performance of such remedial work,

and any failure of the Supplier to comply with its obligations under Clause 5.7(a) or Clause 5.7(b) within the specified or agreed timeframe shall constitute a Notifiable Default.

Specially Written Software warranty

5.8 Without prejudice to Clauses 5.5 (*Supplier Covenants*) and 5.7 (*Services*) and any other rights and remedies of the Authority howsoever arising, the Supplier warrants to the Authority that all components of the Specially Written Software shall:

- (a) be free from material design and programming errors;
- (b) perform in all material respects in accordance with the relevant specifications contained in the Supplier Solution and Documentation; and
- (c) not infringe any Intellectual Property Rights.

Continuing obligation to provide the Services

5.9 The Supplier shall continue to perform all of its obligations under this Contract and shall not suspend the supply of the Services, notwithstanding:

- (a) any withholding of the Service Charges by the Authority pursuant to Clause 7.2(d)(ii) (*Performance Failures*);
- (b) the existence of an unresolved Dispute; and/or
- (c) any failure by the Authority to pay any Charges,

unless the Supplier is entitled to terminate this Contract under Clause 31.3(a) (*Termination by the Supplier*) for failure to pay undisputed Charges.

Optional Services

5.10 The Authority may require the Supplier to provide any or all of the Optional Services at any time by giving notice to the Supplier in writing. The Supplier acknowledges that the Authority is not obliged to take any Optional Services from the Supplier and that nothing shall prevent the Authority from receiving services that are the same as or similar to the Optional Services from any third party.

5.11 If a Change Request is submitted, the Supplier shall, as part of the Impact Assessment provided by the Supplier in relation to such Change Request, provide details of the impact (if any) that the proposed Change will have on the

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

relevant Optional Services.

5.12 Following receipt of the Authority's notice pursuant to Clause 5.10:

- (a) the Parties shall document the inclusion of the relevant Optional Services within the Services in accordance with the Change Control Procedure, modified to reflect the fact that the terms and conditions on which the Supplier shall provide the relevant Optional Services have already been agreed;
- (b) the Supplier shall implement and Test the relevant Optional Services in accordance with the Optional Services Implementation Plan;
- (c) any additional charges for the Optional Services shall be incorporated in the Charges as specified in Paragraph 3 of Part B of Schedule 15 (*Charges and Invoicing*); and
- (d) the Supplier shall, from the date agreed in the Optional Services Implementation Plan (or, if later, the date of Achievement of any Milestones associated with the commencement of the relevant Optional Services (if any)), provide the relevant Optional Services to meet or exceed the applicable Target Performance Level in respect of all Performance Indicators applicable to the Optional Services as set out in Annex 1 of Schedule 3 (*Performance Levels*).

Power of attorney

5.13 By way of security for the performance of its obligations under Clauses 5.5(g) and 5.5(h) (*Supplier covenants*) the Supplier shall use its reasonable endeavours to:

- (a) irrevocably appoints the Authority as its agent and attorney to act with full power and authority in the Supplier's name and on its behalf to do all such acts and execute all such documents as may be necessary or desirable to enforce any such warranties and/or effect any such assignment as are referred to in such Clauses and to delegate one or more of the powers conferred on it by this Clause 5.13 (other than the power to delegate) to officer(s) appointed for that purpose by the Authority and may vary or revoke such delegation at any time;
- (b) promptly, at its own expense, execute any deed that the Authority may reasonably require to create or perfect the appointment of the power of attorney referred to in Clause 5.13(a); and
- (c) ratify and confirm, and agree to ratify and confirm, anything that any of its attorneys may do in the proper and lawful exercise, or purported exercise, of all or any of the rights, powers, authorities and discretions referred to in this Clause 5.13.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Authority Responsibilities

5.14 The Authority shall comply with its responsibilities set out in Schedule 7 (*Authority Responsibilities*).

6 IMPLEMENTATION

Quality Plans

- 6.1 The Supplier shall develop, within forty (40) Working Days of the Effective Date, quality plans that ensure that all aspects of the Services are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it ("**Quality Plans**").
- 6.2 The Supplier shall obtain the Authority Representative's written approval of the Quality Plans before implementing them, which approval shall not be unreasonably withheld or delayed. The Supplier acknowledges and accepts that the Authority's approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Services are provided to the standard required by this Contract.
- 6.3 Following the approval by the Authority of the Quality Plans:
- (a) the Supplier shall design and deliver all Deliverables in accordance with the Quality Plans; and
 - (b) any Changes to the Quality Plans shall be agreed in accordance with the Change Control Procedure.

Implementation Plan and Delays

- 6.4 The Parties shall comply with the provisions of Schedule 13 (*Implementation Plan*) in relation to the agreement and maintenance of the Detailed Implementation Plan.
- 6.5 The Supplier shall:
- (a) comply with the Implementation Plan; and
 - (b) ensure that each Milestone is Achieved on or before its Milestone Date.
- 6.6 If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay:
- (a) it shall:
 - (i) notify the Authority in accordance with Clause 25.1 (*Rectification Plan Process*); and
 - (ii) comply with the Rectification Plan Process in order to address the impact of the Delay or anticipated Delay; and

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (iii) use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay; and
- (b) if the Delay or anticipated Delay relates to a Key Milestone, the provisions of Clause 26 (*Delay Payments*) shall apply.

Testing and Achievement of Milestones

6.7 The Parties shall comply with the provisions of Schedule 14 (*Testing Procedures*) in relation to the procedures to determine whether a Milestone or Test has been Achieved.

7 PERFORMANCE INDICATORS

7.1 The Supplier shall:

- (a) provide the Operational Services in such a manner so as to meet or exceed the Target Performance Level for each Performance Indicator from the date set out in the Implementation Plan; and
- (b) comply with the provisions of Schedule 3 (*Performance Levels*) in relation to the monitoring and reporting on its performance against the Performance Indicators.

Performance Failures

7.2 If in any Service Period:

- (a) a KPI Failure occurs, Service Credits shall be deducted from the Service Charges in accordance with Paragraph 3 of Part C of Schedule 15 (*Charges and Invoicing*);
- (b) a Material KPI Failure occurs, the Supplier shall comply with the Rectification Plan Process (in addition to Service Credits accruing in accordance with Clause 7.2(a));
- (c) a PI Failure occurs, the Supplier shall notify the Authority of the action (if any) it will take to rectify the PI Failure and/or to prevent the PI Failure from recurring; and/or
- (d) a Material PI Failure occurs:
 - (i) the Supplier shall comply with the Rectification Plan Process; and
 - (ii) the Authority may withhold a proportionate amount of the Service Charges in accordance with the process set out in Clause 10.7 (*Set Off and Withholding*) until the relevant Material PI Failure is rectified to the reasonable satisfaction of the Authority, at which point the Authority shall pay the amount withheld.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 7.3 Service Credits shall be the Authority's exclusive financial remedy for a KPI Failure except where:
- (a) the Supplier has accrued Service Credits in excess of the Service Credit Cap in more than six of the Service Periods during the 12 month period immediately preceding the occurrence of the relevant KPI Failure;
 - (b) the KPI Failure:
 - (i) breaches the relevant KPI Service Threshold;
 - (ii) has arisen due to the wilful default by the Supplier or any Supplier Personnel; or
 - (iii) results in:
 - (A) the corruption or loss of any Authority Data (in which case the remedies under Clause 18.7 (*Authority Data and Security Requirements*) shall also be available); and/or
 - (B) the Authority being required to make a compensation payment to one or more third parties;
 - (c) the Supplier has fraudulently misreported its performance against any Performance Indicator; and/or
 - (d) the Authority is otherwise entitled to or does terminate the relevant Services or this Contract pursuant to Clause 31.1(b) (*Termination by the Authority*).

Unacceptable KPI Failure

- 7.4 If in any Service Period an Unacceptable KPI Failure occurs:

- (a) the Authority shall (subject to the limit on liability set out in Clause 23.4(c)(ii)) be entitled to withhold and retain as compensation for the Unacceptable KPI Failure a sum equal to any Service Charges which would otherwise have been due to the Supplier in respect of that Service Period (such sum being "**Compensation for Unacceptable KPI Failure**"); and
- (b) if the Authority withholds and retains such Compensation for Unacceptable KPI Failure, any Service Points and Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue,

provided that the operation of this Clause 7.4 shall be without prejudice to any right which the Authority may have to terminate this Contract and/or to claim damages from the Supplier as a result of such Unacceptable KPI Failure.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

7.5 The Supplier:

- (a) agrees that the application of Clause 7.4 is commercially justifiable where an Unacceptable KPI Failure occurs; and
- (b) acknowledges that it has taken legal advice on the application of Clause 7.4 and has had the opportunity to price for that risk when calculating the Service Charges.

Critical Performance Failure

7.6 If a Critical Performance Failure occurs, the Authority may exercise its rights to terminate this Contract in whole or in part pursuant to Clause 31.1 or 31.2 (*Termination by the Authority*).

Changes to Performance Indicators and Service Credits

7.7 Not more than once in each Contract Year the Authority may, on giving the Supplier at least 3 months' notice:

- (a) change the Service Points that apply in respect of one or more specific Key Performance Indicators; and/or
- (b) convert one or more:
 - (i) Key Performance Indicators into a Subsidiary Performance Indicator; and/or
 - (ii) Subsidiary Performance Indicators into a Key Performance Indicator (in which event the Authority shall also set out in the notice details of what will constitute a Minor KPI Failure, a Serious KPI Failure and a Severe KPI Failure for the new Key Performance Indicator).

7.8 The Supplier shall not be entitled to object to any changes made by the Authority under Clause 7.7, or increase the Service Charges as a result of such changes provided that:

- (a) the total number of Key Performance Indicators does not exceed 20;
- (b) the principal purpose of the change is to reflect changes in the Authority's business requirements and/or priorities or to reflect changing industry standards; and
- (c) there is no change to the Service Credit Cap.

8 SERVICES IMPROVEMENT

8.1 The Supplier shall have an ongoing obligation throughout the Term to identify new or potential improvements to the Services in accordance with this Clause 8. As part of this obligation the Supplier shall identify and report to the Joint Strategic Partnership Board once every 12 months on:

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (a) the emergence of new and evolving relevant technologies which could improve the IT Environment and/or the Services, and those technological advances potentially available to the Supplier and the Authority which the Parties may wish to adopt;
 - (b) new or potential improvements to the Services including the quality, responsiveness, procedures, benchmarking methods, likely performance mechanisms and customer support services in relation to the Services;
 - (c) new or potential improvements to the interfaces or integration of the Services with other services provided by third parties or the Authority which might result in efficiency or productivity gains or reduction of operational risk;
 - (d) changes in business processes and ways of working that would enable the Services to be delivered at lower cost and/or with greater benefits to the Authority; and/or
 - (e) changes to the IT Environment, business processes and ways of working that would enable reductions in the total energy consumed in the delivery of Services.
- 8.2 The Supplier shall ensure that the information that it provides to the Authority shall be sufficient for the Authority to decide whether any improvement should be implemented. The Supplier shall provide any further information that the Authority requests.
- 8.3 If the Authority wishes to incorporate any improvement identified by the Supplier the Authority shall send the Supplier a Change Request in accordance with the Change Control Procedure.

9 EQUIPMENT AND MAINTENANCE

Supplier Equipment

- 9.1 The Supplier shall be solely responsible for the cost of carriage of Supplier Equipment to the Sites and to the Authority Premises, including its off-loading, removal of all packaging and all other associated costs. Likewise on termination or expiry of this Contract the Supplier shall be responsible for the removal and safe disposal of all relevant Supplier Equipment from the Sites and the Authority Premises, including the cost of packing, carriage and making good the Sites and/or the Authority Premises following removal, and taking account of any sustainability requirements, including safe removal of data and recycling requirements.
- 9.2 All the Supplier's property, including Supplier Equipment, shall remain at the sole risk and responsibility of the Supplier, except that the Authority shall be liable for loss of or damage to any of the Supplier's property located on Authority Premises which is due to the negligent act or omission of the Authority.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 9.3 Subject to any express provision of the Service Continuity Plan to the contrary, the loss or destruction for any reason of any Supplier Equipment shall not relieve the Supplier of its obligation to supply the Services in accordance with this Contract, including the Target Performance Levels.

Maintenance

- 9.4 The Supplier shall create and maintain a rolling schedule of planned maintenance to the IT Environment (the "**Maintenance Schedule**") which shall be agreed with the Authority. Once the Maintenance Schedule has been agreed with the Authority Representative, the Supplier shall only undertake such planned maintenance (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule.
- 9.5 The Supplier shall give as much notice as is reasonably practicable to the Authority Representative prior to carrying out any Emergency Maintenance.
- 9.6 The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the IT Environment or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the IT Environment and the Services.

Supply of Goods

- 9.7 Where, as part of the Services, the Supplier is to sell goods or equipment ("**Goods**") to the Authority:
- (a) the relevant Goods and their prices shall be as set out in the Product and Service Catalogue;
 - (b) the Supplier shall supply and, where relevant, install the Goods in accordance with the relevant specification;
 - (c) the Supplier shall ensure that the Goods are free from material defects in design, materials and workmanship and remain so for 12 months after delivery;
 - (d) if following inspection or testing the Authority considers that the Goods do not conform with the relevant specification, the Authority shall inform the Supplier and the Supplier shall immediately take such remedial action as is necessary to ensure compliance;
 - (e) without prejudice to any other rights or remedies of the Authority:
 - (i) risk in the Goods shall pass to the Authority at the time of delivery; and
 - (ii) ownership of the Goods shall pass to the Authority at the time of payment.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (f) the Supplier indemnifies the Authority against the costs of any Recall of the Goods and shall give notice of actual or anticipated action about the Recall of the Goods; and
- (g) the Authority will not be liable for any actions, claims and Losses incurred by the Supplier or any third party during Delivery of the Goods unless and to the extent that it is caused by negligence or other wrongful act of the Authority or its servant or agent. If the Authority suffers or incurs any Loss or injury (whether fatal or otherwise) occurring in the course of Delivery or installation then the Supplier shall indemnify the Authority from any losses, charges, costs or expenses which arise as a result of or in connection with such Loss or injury where it is attributable to any act or omission of the Supplier or any of its Subcontractors or Supplier Personnel.

Transferring Agreements

- 9.8 With effect from the applicable Agreed Transfer Date the Authority shall, subject to Clause 9.9, terminate the Transferring Agreements and the Supplier shall enter into its own contractual arrangements to replace the services and equipment within the scope of the Transferring Agreements. The Parties shall, acting reasonably and with no undue delay, agree the effect of any Change necessitated by the transfer of responsibility for services and equipment within the scope of the Transferring Agreements, as set out in this Clause 9.8, in accordance with the Change Control Procedure, including the effect such transfer may have on the Services, the Supplier meeting the Target Performance Levels and the Charges.
- 9.9 The Parties shall use reasonable endeavours to transfer responsibility for each of the Transferring Agreements to the Supplier as set out in Clause 9.8 with effect from the applicable Agreed Transfer Date. If any consent of any third party is required to give effect to such transfer of responsibility and has not been obtained at or prior to the applicable Agreed Transfer Date, the Authority and the Supplier shall each use all reasonable endeavours to obtain that consent as soon as possible after the applicable Agreed Transfer Date. Unless or until such transfer of responsibility for any Transferring Agreement has occurred, the Parties shall work together, in good faith, to agree an alternative solution which may include the Parties agreeing to novate the benefit of the Transferring Agreements to the Supplier (subject to the burden attaching to each of them), the Supplier finding an alternative source of supply and/or the Parties entering into a Managed Agency Agreement for each applicable Transferring Agreement in substantially the same form as set out in Part B of Schedule 11 (Third Party Contracts).

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SECTION C – PAYMENT, TAXATION AND VALUE FOR MONEY PROVISIONS**10 FINANCIAL AND TAXATION MATTERS****Charges and Invoicing**

- 10.1 In consideration of the Supplier carrying out its obligations under this Contract, including the provision of the Services, the Authority shall pay the Charges to the Supplier in accordance with the pricing and payment profile and the invoicing procedure specified in Schedule 15 (*Charges and Invoicing*).
- 10.2 Except as otherwise provided, each Party shall each bear its own costs and expenses incurred in respect of compliance with its obligations under Clauses 6.7 (*Testing and Achievement of Milestones*), 12 (*Records, Reports, Audits and Open Book Data*), 20 (*Transparency and Freedom of Information*), 21 (*Protection of Personal Data*) and, to the extent specified therein, Clause 27 (*Remedial Adviser*) and Clause 28 (*Step-In Rights*).
- 10.3 If the Authority fails to pay any undisputed Charges properly invoiced under this Contract, the Supplier shall have the right to charge interest on the overdue amount at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgment.

VAT

- 10.4 The Charges are stated exclusive of VAT, which shall be added at the prevailing rate as applicable and paid by the Authority following delivery of a valid VAT invoice.
- 10.5 The Supplier shall indemnify the Authority on a continuing basis against any liability, including any interest, penalties or costs incurred, that is levied, demanded or assessed on the Authority at any time in respect of the Supplier's failure to account for or to pay any VAT relating to payments made to the Supplier under this Contract. Any amounts due under this Clause 10.5 shall be paid in cleared funds by the Supplier to the Authority not less than five Working Days before the date upon which the tax or other liability is payable by the Authority.

Set-off and Withholding

- 10.6 The Authority may set off any amount owed by the Supplier to the Crown or any part of the Crown (including the Authority) against any amount due to the Supplier under this Contract or under any other agreement between the Supplier and the Authority.
- 10.7 If the Authority wishes to:
- (a) set off any amount owed by the Supplier to the Crown or any part of the Crown (including the Authority) against any amount due to the Supplier pursuant to Clause 10.6; or

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) exercise its right pursuant to Clause 7.2(d)(ii) (*Performance Failures*) to withhold payment of a proportion of the Service Charges,

it shall give notice to the Supplier within thirty (30) days of receipt of the relevant invoice, setting out the Authority's reasons for withholding or retaining the relevant Charges.

Benchmarking

- 10.8 The Parties shall comply with the provisions of Schedule 17 (*Benchmarking*) in relation to the benchmarking of any or all of the Services.

Financial Distress

- 10.9 The Parties shall comply with the provisions of Schedule 18 (*Financial Distress*) in relation to the assessment of the financial standing of the Supplier and other specified entities and the consequences of a change to that financial standing.

Promoting Tax Compliance

- 10.10 If, at any point during the Term, an Occasion of Tax Non-Compliance occurs, the Supplier shall:
 - (a) notify the Authority in writing of such fact within 5 Working Days of its occurrence; and
 - (b) promptly provide to the Authority:
 - (i) details of the steps which the Supplier is taking to address the Occasion of Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant; and
 - (ii) such other information in relation to the Occasion of Tax Non-Compliance as the Authority may reasonably require.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SECTION D – CONTRACT GOVERNANCE**11 GOVERNANCE**

11.1 The Parties shall comply with the provisions of Schedule 21 (*Governance*) in relation to the management and governance of this Contract.

Representatives

11.2 Each Party shall have a representative for the duration of this Contract who shall have the authority to act on behalf of their respective Party on the matters set out in, or in connection with, this Contract.

11.3 The initial Supplier Representative shall be the person named as such in Schedule 29 (*Key Personnel*). Any change to the Supplier Representative shall be agreed in accordance with Clause 14 (*Supplier Personnel*).

11.4 The Authority shall notify the Supplier of the identity of the initial Authority Representative within 5 Working Days of the Effective Date. The Authority may, by written notice to the Supplier, revoke or amend the authority of the Authority Representative or appoint a new Authority Representative.

12 RECORDS, REPORTS, AUDITS & OPEN BOOK DATA

12.1 The Supplier shall comply with the provisions of:

- (a) Schedule 24 (*Reports and Records Provisions*) in relation to the maintenance and retention of Records; and
- (b) Part A of Schedule 19 (*Financial Reports and Audit Rights*) in relation to the maintenance of Open Book Data.

12.2 The Parties shall comply with the provisions of:

- (a) Part B of Schedule 19 (*Financial Reports and Audit Rights*) in relation to the provision of the Financial Reports; and
- (b) Part C of Schedule 19 (*Financial Reports and Audit Rights*) in relation to the exercise of the Audit Rights by the Authority or any Audit Agents.

13 CHANGE**Change Control Procedure, Service Requests and Projects**

13.1 Any requirement for a Change shall be subject to the Change Control Procedure. Any requirement for a Service Request or a Project shall be subject to the procedures set out in Part B of Schedule 22 (Change Control Procedure, Service Requests and Projects).

Change in Law

13.2 The Supplier shall neither be relieved of its obligations to supply the Services in accordance with the terms and conditions of this Contract nor be entitled to an

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

increase in the Charges as the result of:

- (a) a General Change in Law; or
- (b) a Specific Change in Law where the effect of that Specific Change in Law on the Services is reasonably foreseeable at the Effective Date.

13.3 If a Specific Change in Law occurs or will occur during the Term (other than as referred to in Clause 13.2(b)), the Supplier shall:

- (a) notify the Authority as soon as reasonably practicable of the likely effects of that change, including:
 - (i) whether any Change is required to the Services, the Charges or this Contract; and
 - (ii) whether any relief from compliance with the Supplier's obligations is required, including any obligation to Achieve a Milestone and/or to meet the Target Performance Levels; and
- (b) provide the Authority with evidence:
 - (i) that the Supplier has minimised any increase in costs or maximised any reduction in costs, including in respect of the costs of its Sub-contractors;
 - (ii) as to how the Specific Change in Law has affected the cost of providing the Services; and
 - (iii) demonstrating that any expenditure that has been avoided, for example which would have been required under the provisions of Clause 8 (*Services Improvement*), has been taken into account in amending the Charges.

13.4 Any variation in the Charges or relief from the Supplier's obligations resulting from a Specific Change in Law (other than as referred to in Clause 13.2(b)) shall be implemented in accordance with the Change Control Procedure.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SECTION E – SUPPLIER PERSONNEL AND SUPPLY CHAIN**14 SUPPLIER PERSONNEL****14.1 The Supplier shall:**

- (a) provide in advance of any admission to Authority Premises a list of the names of all Supplier Personnel requiring such admission, specifying the capacity in which they require admission and giving such other particulars as the Authority may reasonably require;
- (b) ensure that all Supplier Personnel:
 - (i) are appropriately qualified, trained and experienced to provide the Services with all reasonable skill, care and diligence;
 - (ii) are vetted in accordance with Good Industry Practice and, where applicable, the security requirements set out in Schedule 2 (*Services Description*) and the “MoJ Cyber and Technical Security Guidance”; and
 - (iii) comply with all reasonable requirements of the Authority concerning conduct at the Authority Premises, including the Standards;
- (c) subject to Schedule 28 (*Staff Transfer*), retain overall control of the Supplier Personnel at all times so that the Supplier Personnel shall not be deemed to be employees, agents or contractors of the Authority;
- (d) be liable at all times for all acts or omissions of Supplier Personnel, so that any act or omission of a member of any Supplier Personnel which results in a Default under this Contract shall be a Default by the Supplier;
- (e) use all reasonable endeavours to minimise the number of changes in Supplier Personnel;
- (f) replace (temporarily or permanently, as appropriate) any Supplier Personnel as soon as practicable if any Supplier Personnel have been removed or are unavailable for any reason whatsoever;
- (g) bear the programme familiarisation and other costs associated with any replacement of any Supplier Personnel; and
- (h) procure that the Supplier Personnel shall vacate the Authority Premises immediately upon the termination or expiry of this Contract.

14.2 If the Authority reasonably believes that any of the Supplier Personnel are unsuitable to undertake work in respect of this Contract, it may:

- (a) refuse admission to the relevant person(s) to the Authority Premises; and/or

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) direct the Supplier to end the involvement in the provision of the Services of the relevant person(s).

Key Personnel

- 14.3 The Supplier shall ensure that the Key Personnel fulfil the Key Roles at all times during the Term. Schedule 29 (*Key Personnel*) lists the Key Roles and names of the persons who the Supplier shall appoint to fill those Key Roles at the Effective Date.
- 14.4 The Authority may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Personnel.
- 14.5 The Supplier shall not remove or replace any Key Personnel (including when carrying out Exit Management) unless:
 - (a) requested to do so by the Authority;
 - (b) the person concerned resigns, retires or dies or is on maternity leave, paternity leave or shared parental leave or long-term sick leave;
 - (c) the person's employment or contractual arrangement with the Supplier or a Sub-contractor is terminated for material breach of contract by the employee; or
 - (d) the Supplier obtains the Authority's prior written consent (such consent not to be unreasonably withheld or delayed).
- 14.6 The Supplier shall:
 - (a) notify the Authority promptly of the absence of any Key Personnel (other than for short-term sickness or holidays of 2 weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);
 - (b) ensure that any Key Role is not vacant for any longer than 10 Working Days;
 - (c) give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Personnel and, except in the cases of death, unexpected ill health or a material breach of the Key Personnel's employment contract, this will mean at least 60 Working Days' notice;
 - (d) ensure that all arrangements for planned changes in Key Personnel provide adequate periods during which incoming and outgoing personnel work together to transfer responsibilities and ensure that such change does not have an adverse impact on the performance of the Services; and
 - (e) ensure that any replacement for a Key Role:

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (i) has a level of qualifications and experience appropriate to the relevant Key Role; and
- (ii) is fully competent to carry out the tasks assigned to the Key Personnel whom they have replaced.

Employment Indemnity

14.7 The Parties agree that:

- (a) the Supplier shall both during and after the Term indemnify the Authority against all Employee Liabilities that may arise as a result of any claims brought against the Authority by any person where such claim arises from any act or omission of the Supplier or any Supplier Personnel; and
- (b) the Authority shall both during and after the Term indemnify the Supplier against all Employee Liabilities that may arise as a result of any claims brought against the Supplier by any person where such claim arises from any act or omission of the Authority or any of the Authority's employees, agents, consultants and contractors.

Income Tax and National Insurance Contributions

14.8 Where the Supplier or any Supplier Personnel are liable to be taxed in the UK or to pay national insurance contributions in respect of consideration received under this Contract, the Supplier shall:

- (a) at all times comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, and the Social Security Contributions and Benefits Act 1992 and all other statutes and regulations relating to national insurance contributions, in respect of that consideration; and
- (b) indemnify the Authority against any income tax, national insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made in connection with the provision of the Services by the Supplier or any Supplier Personnel.

Staff Transfer

14.9 The Parties agree that:

- (a) where the commencement of the provision of the Services or any part of the Services results in one or more Relevant Transfers, Schedule 28 (*Staff Transfer*) shall apply as follows:
 - (i) where the Relevant Transfer involves the transfer of Transferring Authority Employees, Part D of Schedule 28 (*Staff Transfer*) shall apply;

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (ii) where the Relevant Transfer involves the transfer of Transferring Former Supplier Employees, Part B and Part D of Schedule 28 (*Staff Transfer*) shall apply;
- (iii) where the Relevant Transfer involves the transfer of Transferring Authority Employees and Transferring Former Supplier Employees, Parts B and D of Schedule 28 (*Staff Transfer*) shall apply; and
- (iv) Part C of Schedule 28 (*Staff Transfer*) shall not apply;
- (b) where commencement of the provision of the Services or a part of the Services does not result in a Relevant Transfer, Part C of Schedule 28 (*Staff Transfer*) shall apply, Part D of Schedule 28 may apply and Part B of Schedule 28 (*Staff Transfer*) shall not apply; and
- (c) Part E of Schedule 28 (*Staff Transfer*) shall apply on the expiry or termination of the Services or any part of the Services.

15 SUPPLY CHAIN RIGHTS AND PROTECTIONS**Advertising Sub-contract Opportunities**

15.1 The Supplier shall:

- (a) subject to Clauses 15.3 and 15.4, advertise on Contracts Finder all Sub-contract opportunities arising from or in connection with the provision of the Goods and/or Services and/or Works above a minimum threshold of £25,000 that arise during the Term;
- (b) within ninety (90) days of awarding a Sub-contract to a Sub-contractor, update the notice on Contracts Finder with details of the successful Sub-contractor;
- (c) monitor the number, type and value of the Sub-contract opportunities placed on Contracts Finder advertised and awarded in its supply chain during the Term;
- (d) provide reports on the information at Clause 15.1(c) to the Authority in the format and frequency as reasonably specified by the Authority; and
- (e) promote Contracts Finder to its suppliers and encourage those organisations to register on Contracts Finder.

15.2 Each advert referred to in Clause 15.1 above shall provide a full and detailed description of the Sub-contract opportunity with each of the mandatory fields being completed on Contracts Finder by the Supplier.

15.3 The obligation at Clause 15.1 shall only apply in respect of Sub-contract opportunities arising after the Effective Date.

15.4 Notwithstanding Clause 15.1 the Authority may, by giving its prior written

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

approval, agree that a Sub-contract opportunity is not required to be advertised on Contracts Finder.

Appointment of Sub-contractors

- 15.5 The Supplier shall exercise due skill and care in the selection and appointment of any Sub-contractors to ensure that the Supplier is able to:
- (a) manage any Sub-contractors in accordance with Good Industry Practice;
 - (b) comply with its obligations under this Contract in the delivery of the Services; and
 - (c) assign, novate or otherwise transfer to the Authority or any Replacement Supplier any of its rights and/or obligations under each Sub-contract that relates exclusively to this Contract.
- 15.6 Prior to sub-contracting any of its obligations under this Contract, the Supplier shall notify the Authority in writing of:
- (a) the proposed Sub-contractor's name, registered office and company registration number;
 - (b) the scope of any Services to be provided by the proposed Sub-contractor; and
 - (c) where the proposed Sub-contractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of the Authority that the proposed Sub-contract has been agreed on "arm's-length" terms.
- 15.7 If requested by the Authority within 10 Working Days of receipt of the Supplier's notice issued pursuant to Clause 15.6, the Supplier shall also provide:
- (a) a copy of the proposed Sub-contract; and
 - (b) any further information reasonably requested by the Authority.
- 15.8 The Authority may, within 10 Working Days of receipt of the Supplier's notice issued pursuant to Clause 15.6 (or, if later, receipt of any further information requested pursuant to Clause 15.7), object to the appointment of the relevant Sub-contractor if it considers that:
- (a) the appointment of a proposed Sub-contractor may prejudice the provision of the Services and/or may be contrary to the interests of the Authority;
 - (b) the proposed Sub-contractor is unreliable and/or has not provided reasonable services to its other customers;
 - (c) the proposed Sub-contractor employs unfit persons; and/or

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (d) the proposed Sub-contractor should be excluded in accordance with Clause 15.222 (*Termination of sub-contracts*);

in which case, the Supplier shall not proceed with the proposed appointment.

15.9 If:

- (a) the Authority has not notified the Supplier that it objects to the proposed Sub-contractor's appointment by the later of 10 Working Days of receipt of:
- (i) the Supplier's notice issued pursuant to Clause 15.6; and
 - (ii) any further information requested by the Authority pursuant to Clause 15.7; and
- (b) the proposed Sub-contract is not a Key Sub-contract (which shall require the written consent of the Authority in accordance with Clause 15.10 (*Appointment of Key Sub-contractors*),

the Supplier may proceed with the proposed appointment and, where the Sub-contract is entered into exclusively for the purpose of delivery of the Services, may notify the Authority that the relevant Sub-contract shall constitute a Third Party Contract for the purposes of Part A of Schedule 11 (*Third Party Contracts*).

Appointment of Key Sub-contractors

15.10 Where the Supplier wishes to enter into a Key Sub-contract or replace a Key Sub-contractor, it must obtain the prior written consent of the Authority, such consent not to be unreasonably withheld or delayed. For these purposes, the Authority may withhold its consent to the appointment of a Key Sub-contractor if it reasonably considers that:

- (a) the appointment of a proposed Key Sub-contractor may prejudice the provision of the Services or may be contrary to the interests of the Authority;
- (b) the proposed Key Sub-contractor is unreliable and/or has not provided reasonable services to its other customers; and/or
- (c) the proposed Key Sub-contractor employs unfit persons; and/or
- (d) the proposed Key Sub-contractor should be excluded in accordance with Clause 15.22 (*Termination of sub-contracts*).

15.11 The Authority consents to the appointment of the Key Sub-contractors listed in Schedule 10 (*Notified Key Sub-contractors*).

15.12 Except where the Authority has given its prior written consent, the Supplier shall ensure that each Key Sub-contract shall include:

- (a) provisions which will enable the Supplier to discharge its obligations under this Contract;

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) a right under CRTPA for the Authority to enforce any provisions under the Key Sub-contract which are capable of conferring a benefit upon the Authority;
- (c) a provision enabling the Authority to enforce the Key Sub-contract as if it were the Supplier;
- (d) a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-contract to the Authority or any Replacement Supplier without restriction (including any need to obtain any consent or approval) or payment by the Authority;
- (e) obligations no less onerous on the Key Sub-contractor than those imposed on the Supplier under this Contract in respect of:
 - (i) data protection requirements set out in Clauses 18 (*Authority Data and Security Requirements*) and 21 (*Protection of Personal Data*);
 - (ii) FOIA requirements set out in Clause 20 (*Transparency and Freedom of Information*);
 - (iii) the obligation not to embarrass the Authority or otherwise bring the Authority into disrepute set out in Clause 5.5(m) (*Services*);
 - (iv) the keeping of records in respect of the services being provided under the Key Sub-contract, including the maintenance of Open Book Data; and
 - (v) the conduct of Audits set out in Part C of Schedule 19 (*Financial Reports and Audit Rights*);
- (f) provisions enabling the Supplier to terminate the Key Sub-contract on notice on terms no more onerous on the Supplier than those imposed on the Authority under Clauses 31.1(a) (*Termination by the Authority*), 31.1A (*Partial Termination for Convenience*) and 32.5 (*Payments by the Authority*) and Schedule 16 (*Payments on Termination*) of this Contract;
- (g) a provision restricting the ability of the Key Sub-contractor to sub-contract all or any part of the services provided to the Supplier under the Key Sub-contract without first seeking the written consent of the Authority;
- (h) a provision enabling the Supplier or the Authority to appoint a Remedial Adviser on substantially the same terms as are set out in Clause 27 (*Remedial Adviser*);
- (i) a provision enabling the Supplier, the Authority or any other person on behalf of the Authority to step-in on substantially the same terms as are set out in Clause 28 (*Step-in Rights*);

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (j) a provision requiring the Key Sub-contractor to participate in, and if required by the Authority in the relevant Multi-Party Procedure Initiation Notice to procure the participation of all or any of its Sub-contractors in, the Multi-Party Dispute Resolution Procedure; and
- (k) a provision requiring the Key Sub-contractor to:
 - (i) promptly notify the Supplier and the Authority in writing of any of the following of which it is, or ought to be, aware:
 - (A) the occurrence of a Financial Distress Event in relation to the Key Sub-contractor; or
 - (B) any fact, circumstance or matter of which it is aware which could cause the occurrence of a Financial Distress Event in relation to the Key Sub-contractor,

and in any event, provide such notification within 10 Working Days of the date on which the Key Sub-contractor first becomes aware of such); and
 - (ii) co-operate with the Supplier and the Authority in order to give full effect to the provisions of Schedule 18 (*Financial Distress*), including meeting with the Supplier and the Authority to discuss and review the effect of the Financial Distress Event on the continued performance and delivery of the Services, and contributing to and complying with the Financial Distress Remediation Plan, and providing the information specified at Paragraph 4.3(b)(ii) of Schedule 18 (*Financial Distress*).

15.13 The Supplier shall not terminate or materially amend the terms of any Key Sub-contract without the Authority's prior written consent, which shall not be unreasonably withheld or delayed.

Supply chain protection

15.14 For Sub-contracts in the Supplier's supply chain made wholly or substantially for the purpose of performing or contributing to the performance of the whole or any part of this Contract:

- (a) where such Sub-Contracts are entered into after the Effective Date, the Supplier will ensure that they all contain provisions that; or
- (b) where such Sub-Contracts are entered into before the Effective Date, the Supplier will take all reasonable endeavours to ensure that they all contain provisions that:
 - (i) give the Supplier a right to terminate the Sub-contract if the Sub-contractor fails to comply in the performance of the Sub-contract with legal obligations in the fields of environmental, social or labour Law;

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (ii) require the Supplier or other party receiving goods or services under the contract to consider and verify invoices under that contract in a timely fashion;
- (c) if the Supplier or other party fails to consider and verify an invoice in accordance with Clause 15.14(b)(ii), the invoice shall be regarded as valid and undisputed for the purpose of Clause 15.14(d) after a reasonable time has passed;
- (d) require the Supplier or other party to pay any undisputed sums which are due from it to the Sub-contractor within a specified period not exceeding thirty (30) days of verifying that the invoice is valid and undisputed;
- (e) give the Authority a right to publish the Supplier's compliance with its obligation to pay undisputed invoices within the specified payment period; and
- (f) require the Sub-contractor to include a clause to the same effect as this Clause 15.14 in any contracts it enters into wholly or substantially for the purpose of performing or contributing to the performance of the whole or any part of this Contract.

15.15 The Supplier shall:

- (a) pay any undisputed sums which are due from it to a Sub-contractor within thirty (30) days of verifying that the invoice is valid and undisputed;
- (b) include within the Balanced Scorecard Report produced by it pursuant to Schedule 3 (*Performance Levels*) a summary of its compliance with Clause 15.15(a), such data to be certified each Quarter by a director of the Supplier as being accurate and not misleading.

15.16 Without prejudice to Clause 15.15(a), the Supplier shall:

- (a) pay any sums which are due from it to any Sub-contractor or Unconnected Sub-contractor pursuant to any invoice (or other notice of an amount for payment) on the earlier of:
 - (i) the date set out for payment in the relevant Sub-contract or Unconnected Sub-contract; or
 - (ii) the date that falls sixty (60) days after the day on which the Supplier receives an invoice (or otherwise has notice of an amount for payment); and
- (b) include within the Balanced Scorecard Report produced by it pursuant to Schedule 3 (*Performance Levels*) a summary of its compliance with Clause 15.16(a), such data to be certified every six

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

months by a director of the Supplier as being accurate and not misleading.

15.17 If any Balanced Scorecard Report shows that in either of the last two six month periods the Supplier failed to pay 95% or above of all Sub-contractor or Unconnected Sub-contractor invoices (or other notice of an amount for payment) within sixty (60) days of receipt, the Supplier shall upload to the Virtual Library within 15 Working Days of submission of the latest Balanced Scorecard Report an action plan (the “**Action Plan**”) for improvement. The Action Plan shall include, but not be limited to, the following:

- (a) identification of the primary causes of failure to pay 95% or above of all Sub-contractor or Unconnected Sub-contractor invoices (or other notice of an amount for payment) within sixty (60) days of receipt;
- (b) actions to address each of the causes set out in Clause 15.17(a); and
- (c) mechanism for and commitment to regular reporting on progress to the Supplier’s Board.

15.18 The Action Plan shall be certificated by a director of the Supplier and the Action Plan or a summary of the Action Plan published on the Supplier’s website within 10 Working Days of the date on which the Action Plan is uploaded to the Virtual Library.

15.19 Where the Supplier fails to pay any sums due to any Sub-contractor or Unconnected Sub-contractor in accordance with the terms set out in the relevant Sub-contract or Unconnected Sub-contract, the Action Plan shall include details of the steps the Supplier will take to address this.

15.20 The Supplier shall comply with the Action Plan or any similar action plan connected to the payment of Sub-contractors or Unconnected Sub-contractors which is required to be submitted to the Authority as part of the procurement process and such action plan shall be included as part of the Supplier’s Solution (to the extent it is not already included).

15.21 Notwithstanding any provision of Clauses 19 (*Confidentiality*) and 22 (*Publicity and Branding*), if the Supplier notifies the Authority (whether in a Balanced Scorecard Report or otherwise) that the Supplier has failed to pay a Sub-contractor’s undisputed invoice within thirty (30) days of receipt or that it has failed to pay 95% or above of its Sub-Contractors or Unconnected Sub-contractors within sixty (60) days after the day on which the Supplier receives an invoice or otherwise has notice of an amount for payment, or the Authority otherwise discovers the same, the Authority shall be entitled to publish the details of the late or non-payment (including on government websites and in the press).

Termination of Sub-contracts

15.22 The Authority may require the Supplier to terminate:

- (a) a Sub-contract where:

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (i) the acts or omissions of the relevant Sub-contractor have caused or materially contributed to the Authority's right of termination pursuant to Clause 31.1(b) (*Termination by the Authority*);
 - (ii) the relevant Sub-contractor or any of its Affiliates have embarrassed the Authority or otherwise brought the Authority into disrepute by engaging in any act or omission which is reasonably likely to diminish the trust that the public places in the Authority, regardless of whether or not such act or omission is related to the Sub-contractor's obligations in relation to the Services or otherwise;
 - (iii) the relevant Sub-contractor has failed to comply in the performance of its Sub-contract with legal obligations in the fields of environmental, social or labour law; and/or
 - (iv) the Authority has found grounds for exclusion of the Sub-contractor in accordance with Clause 15.26; and
- (b) a Key Sub-contract where there is a change of Control of the relevant Key Sub-contractor, unless:
- (i) the Authority has given its prior written consent to the particular change of Control, which subsequently takes place as proposed; or
 - (ii) the Authority has not served its notice of objection within 6 months of the later of the date the change of Control took place or the date on which the Authority was given notice of the change of Control.

Competitive Terms

15.23 If the Authority is able to obtain from any Sub-contractor or any other third party (on a like-for-like basis) more favourable commercial terms with respect to the supply of any goods, software or services used by the Supplier or the Supplier Personnel in the supply of the Services, then the Authority may require the Supplier to replace its existing commercial terms with that person with the more favourable commercial terms obtained by the Authority in respect of the relevant item.

15.24 If the Authority exercises its option pursuant to Clause 15.23, then the Charges shall be reduced by an amount that is agreed in accordance with the Change Control Procedure.

Retention of Legal Obligations

15.25 Notwithstanding the Supplier's right to sub-contract pursuant to this Clause 15, the Supplier shall remain responsible for all acts and omissions of its Sub-contractors and the acts and omissions of those employed or engaged by the Sub-contractors as if they were its own. In respect of any element of the

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Services delivered by Supplier Personnel and/or which are Sub-contracted by the Supplier, an obligation on the Supplier to do or to refrain from doing any act or thing under this Contract, shall include an obligation on the Supplier to procure that the Supplier Personnel and the Sub-contractor also do or refrain from doing such act or thing in their delivery of those elements of the Services.

Exclusion of Sub-contractors

15.26 Where the Authority considers whether there are grounds for the exclusion of a Sub-contractor under Regulation 57 of the Public Contracts Regulations 2015, then:

- (a) if the Authority finds there are compulsory grounds for exclusion, the Supplier shall replace or shall not appoint the Sub-contractor;
- (b) if the Authority finds there are non-compulsory grounds for exclusion, the Authority may require the Supplier to replace or not to appoint the Sub-contractor and the Supplier shall comply with such a requirement.

Reporting SME/VCSE Sub-contracts

15.27 In addition to any other Management Information requirements set out in this Contract, the Supplier agrees that it shall, at no charge, provide timely, full, accurate and complete Supply Chain Transparency Reports to the Authority thirty (30) days prior to the end of each financial year by providing all of the information described in the Supply Chain Transparency Information Template in the format set out in the Schedule 24 (*Reports and Records Provisions*) Annex 4 and in accordance with any guidance issued by the Authority from time to time.

15.28 The Authority may update the Supply Chain Transparency Information Template from time to time (including the data required and/or format) by issuing a replacement version with at least thirty (30) days' notice and specifying the date from which it must be used.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SECTION F – INTELLECTUAL PROPERTY, DATA AND CONFIDENTIALITY**16 INTELLECTUAL PROPERTY RIGHTS**

- 16.1 The Parties agree that the terms set out in Schedule 32 (*Intellectual Property Rights*) shall apply to this Contract.

17 IPRs INDEMNITY

- 17.1 The Supplier shall at all times, during and after the Term, on written demand indemnify the Authority and each other Indemnified Person, and keep the Authority and each other Indemnified Person indemnified, against all Losses incurred by, awarded against or agreed to be paid by an Indemnified Person arising from an IPRs Claim.
- 17.2 If an IPRs Claim is made, or the Supplier anticipates that an IPRs Claim might be made, the Supplier may, at its own expense and sole option, either:
- (a) procure for the Authority or other relevant Indemnified Person the right to continue using the relevant item which is subject to the IPRs Claim; or
 - (b) replace or modify the relevant item with non-infringing substitutes provided that:
 - (i) the performance and functionality of the replaced or modified item is at least equivalent to the performance and functionality of the original item;
 - (ii) the replaced or modified item does not have an adverse effect on any other services or the IT Environment;
 - (iii) there is no additional cost to the Authority or relevant Indemnified Person (as the case may be); and
 - (iv) the terms and conditions of this Contract shall apply to the replaced or modified Services.
- 17.3 If the Supplier elects to procure a licence in accordance with Clause 17.2(a) or to modify or replace an item pursuant to Clause 17.2(b), but this has not avoided or resolved the IPRs Claim, then:
- (a) the Authority may terminate this Contract (if subsisting in accordance with Clause 31.1) with immediate effect by written notice to the Supplier; and
 - (b) without prejudice to the indemnity set out in Clause 17.1, the Supplier shall be liable for all reasonable and unavoidable costs of the substitute items and/or services including the additional costs of procuring, implementing and maintaining the substitute items.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

18 AUTHORITY DATA AND SECURITY REQUIREMENTS

- 18.1 The Supplier shall not delete or remove any proprietary notices contained within or relating to the Authority Data.
- 18.2 The Supplier shall not store, copy, disclose, or use the Authority Data except as necessary for the performance by the Supplier of its obligations under this Contract or as otherwise expressly authorised in writing by the Authority.
- 18.3 To the extent that Authority Data is held and/or processed by the Supplier, the Supplier shall supply that Authority Data to the Authority as requested by the Authority in the format specified in Schedule 2 (*Services Description*).
- 18.4 The Supplier shall preserve the integrity of Authority Data and prevent the corruption or loss of Authority Data at all times that the relevant Authority Data is under its control or the control of any Sub-contractor.
- 18.5 The Supplier shall perform secure back-ups of all Authority Data and shall ensure that up-to-date back-ups are stored off-site in accordance with the Service Continuity Plan. The Supplier shall ensure that such back-ups are available to the Authority (or to such other person as the Authority may direct) at all times upon request and are delivered to the Authority at no less than 6 monthly intervals (or such other intervals as may be agreed in writing between the Parties) via a secure encrypted method.
- 18.6 The Supplier shall ensure that any system on which the Supplier holds any Authority Data, including back-up data, is a secure system that complies with the Standards.
- 18.7 If the Authority Data is corrupted, lost or sufficiently degraded as a result of the Supplier's Default so as to be unusable, the Authority may:
- (a) require the Supplier (at the Supplier's expense) to restore or procure the restoration of Authority Data to the extent and in accordance with the requirements specified in Schedule 26 (*Service Continuity Plan and Corporate Resolution Planning*) and the Supplier shall do so as soon as practicable but not later than 5 Working Days from the date of receipt of the Authority's notice; and/or
 - (b) itself restore or procure the restoration of Authority Data, and shall be repaid by the Supplier any reasonable expenses incurred in doing so to the extent and in accordance with the requirements specified in Schedule 26 (*Service Continuity Plan and Corporate Resolution Planning*).
- 18.8 If at any time the Supplier suspects or has reason to believe that Authority Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the Supplier shall notify the Authority immediately and inform the Authority of the remedial action the Supplier proposes to take.
- 18.9 The Supplier shall comply with the requirements of Schedule 5 (*Security Management*).

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 18.10 The Authority shall notify the Supplier of any changes or proposed changes to the Baseline Security Requirements.
- 18.11 If the Supplier believes that a change or proposed change to the Baseline Security Requirements will have a material and unavoidable cost implication to the Services it may submit a Change Request. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall then be agreed in accordance with the Change Control Procedure.
- 18.12 Until and/or unless a change to the Charges is agreed by the Authority pursuant to Clause 18.11 the Supplier shall continue to perform the Services in accordance with its existing obligations.

19 CONFIDENTIALITY

- 19.1 For the purposes of this Clause 19, the term “**Disclosing Party**” shall mean a Party which discloses or makes available directly or indirectly its Confidential Information and “**Recipient**” shall mean the Party which receives or obtains directly or indirectly Confidential Information.
- 19.2 Except to the extent set out in this Clause 19 or where disclosure is expressly permitted elsewhere in this Contract, the Recipient shall:
- (a) treat the Disclosing Party’s Confidential Information as confidential and keep it in secure custody (which is appropriate depending upon the form in which such materials are stored and the nature of the Confidential Information contained in those materials);
 - (b) not disclose the Disclosing Party’s Confidential Information to any other person except as expressly set out in this Contract or without obtaining the owner’s prior written consent;
 - (c) not use or exploit the Disclosing Party’s Confidential Information in any way except for the purposes anticipated under this Contract; and
 - (d) immediately notify the Disclosing Party if it suspects or becomes aware of any unauthorised access, copying, use or disclosure in any form of any of the Disclosing Party’s Confidential Information.
- 19.3 The Recipient shall be entitled to disclose the Confidential Information of the Disclosing Party where:
- (a) the Recipient is required to disclose the Confidential Information by Law, provided that Clause 20 (*Transparency and Freedom of Information*) shall apply to disclosures required under the FOIA or the EIRs;
 - (b) the need for such disclosure arises out of or in connection with:

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (i) any legal challenge or potential legal challenge against the Authority arising out of or in connection with this Contract;
 - (ii) the examination and certification of the Authority's accounts (provided that the disclosure is made on a confidential basis) or for any examination pursuant to section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority is making use of any Services provided under this Contract; or
 - (iii) the conduct of a Crown Body review in respect of this Contract; or
 - (c) the Recipient has reasonable grounds to believe that the Disclosing Party is involved in activity that may constitute a criminal offence under the Bribery Act 2010 and the disclosure is being made to the Serious Fraud Office.
- 19.4 If the Recipient is required by Law to make a disclosure of Confidential Information, the Recipient shall as soon as reasonably practicable and to the extent permitted by Law notify the Disclosing Party of the full circumstances of the required disclosure including the relevant Law and/or regulatory body requiring such disclosure and the Confidential Information to which such disclosure would apply.
- 19.5 The Supplier may disclose the Confidential Information of the Authority on a confidential basis only to:
- (a) Supplier Personnel who are directly involved in the provision of the Services and need to know the Confidential Information to enable performance of the Supplier's obligations under this Contract;
 - (b) its auditors; and
 - (c) its professional advisers for the purposes of obtaining advice in relation to this Contract.
- Where the Supplier discloses Confidential Information of the Authority pursuant to this Clause 19.5, it shall remain responsible at all times for compliance with the confidentiality obligations set out in this Contract by the persons to whom disclosure has been made.
- 19.6 The Authority may disclose the Confidential Information of the Supplier:
- (a) on a confidential basis to any Crown Body for any proper purpose of the Authority or of the relevant Crown Body;
 - (b) to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement;

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (c) to the extent that the Authority (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions;
- (d) on a confidential basis to a professional adviser, consultant, supplier or other person engaged by any of the entities described in Clause 19.6(a) (including any benchmarking organisation) for any purpose relating to or connected with this Contract;
- (e) on a confidential basis for the purpose of the exercise of its rights under this Contract, including the Audit Rights, its step-in rights pursuant to Clause 28 (*Step-In Rights*), its rights to appoint a Remedial Adviser pursuant to Clause 27 (*Remedial Adviser*) and Exit Management rights; or
- (f) on a confidential basis to a proposed Successor Body in connection with any assignment, novation or disposal of any of its rights, obligations or liabilities under this Contract,

and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Authority under this Clause 19.

- 19.7 Nothing in this Clause 19 shall prevent a Recipient from using any techniques, ideas or know-how gained during the performance of this Contract in the course of its normal business to the extent that this use does not result in a disclosure of the Disclosing Party's Confidential Information or an infringement of Intellectual Property Rights.

20 TRANSPARENCY AND FREEDOM OF INFORMATION

- 20.1 The Parties acknowledge that:

- (a) the Transparency Reports;
- (b) the content of this Contract, including any changes to this Contract agreed from time to time, except for –
 - (i) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Authority; and
 - (ii) Commercially Sensitive Information; and
- (c) the Publishable Performance Information

(together the “**Transparency Information**”) are not Confidential Information.

- 20.2 Notwithstanding any other provision of this Contract, the Supplier hereby gives its consent for the Authority to publish to the general public the Transparency Information in its entirety (but with any information which is exempt from disclosure in accordance with the provisions of the FOIA redacted). The

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Authority shall, prior to publication, consult with the Supplier on the manner and format of publication and to inform its decision regarding any redactions but shall have the final decision in its absolute discretion.

- 20.3 The Supplier shall assist and co-operate with the Authority to enable the Authority to publish the Transparency Information, including the preparation of the Transparency Reports in accordance with Paragraph 1 of Schedule 24 (*Reports and Records Provisions*).
- 20.4 If the Authority believes that publication of any element of the Transparency Information would be contrary to the public interest, the Authority shall be entitled to exclude such information from publication. The Authority acknowledges that it would expect the public interest by default to be best served by publication of the Transparency Information in its entirety. Accordingly, the Authority acknowledges that it will only exclude Transparency Information from publication in exceptional circumstances and agrees that where it decides to exclude information from publication it will provide a clear explanation to the Supplier.
- 20.5 The Authority shall publish the Transparency Information in a format that assists the general public in understanding the relevance and completeness of the information being published to ensure the public obtain a fair view on how the Contract is being performed, having regard to the context of the wider commercial relationship with the Supplier.
- 20.6 The Supplier agrees that any Information it holds that is not included in the Transparency Reports but is reasonably relevant to or that arises from the provision of the Services shall be provided to the Authority on request unless the cost of doing so would exceed the appropriate limit prescribed under section 12 of the FOIA. The Authority may disclose such information under the FOIA and the EIRs and may (except for Commercially Sensitive Information, Confidential Information (subject to Clause 19.6(c)) and Open Book Data) publish such Information. The Supplier shall provide to the Authority within five (5) Working Days (or such other period as the Authority may reasonably specify) any such Information requested by the Authority.
- 20.7 The Supplier acknowledges that the Authority is subject to the requirements of the FOIA and the EIRs. The Supplier shall:
- (a) provide all necessary assistance and cooperation as reasonably requested by the Authority to enable the Authority to comply with its obligations under the FOIA and EIRs;
 - (b) transfer to the Authority all Requests for Information relating to this Contract that it receives as soon as practicable and in any event within 2 Working Days of receipt;
 - (c) provide the Authority with a copy of all Information held on behalf of the Authority which is requested in a Request For Information and which is in its possession or control in the form that the Authority requires within 5 Working Days (or such other period as the Authority

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

may reasonably specify) of the Authority's request for such Information; and

- (d) not respond directly to a Request For Information addressed to the Authority unless authorised in writing to do so by the Authority.

20.8 The Supplier acknowledges that the Authority may be required under the FOIA and EIRs to disclose Information (including Commercially Sensitive Information) without consulting or obtaining consent from the Supplier. The Authority shall take reasonable steps to notify the Supplier of a Request For Information (in accordance with the Secretary of State's section 45 Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the FOIA) to the extent that it is permissible and reasonably practical for it to do so but (notwithstanding any other provision in this Contract) the Authority shall be responsible for determining in its absolute discretion whether any Commercially Sensitive Information and/or any other information is exempt from disclosure in accordance with the FOIA and EIRs.

21 PROTECTION OF PERSONAL DATA

21.1 The Supplier shall indemnify the Authority against any and all Losses incurred by the Authority due to breach by the Supplier of Data Protection Legislation or Clause 21.

Status of the Controller

21.2 The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under this Contract will determine the status of each Party under the Data Protection Legislation. A Party may act as:

- (a) "Controller" (where the other Party acts as the "Processor");
- (b) "Processor" (where the other Party acts as the "Controller");
- (c) "Joint Controller" (where both Parties are considered to jointly control the same Personal Data);
- (d) "Independent Controller" of the Personal Data where the other Party is also "Controller" of the same Personal Data in its own right (but there is no element of joint control);

and the Parties shall set out in Schedule 31 (*Processing Personal Data*) which scenario or scenarios are intended to apply under this Contract.

Where one Party is Controller and the other Party its Processor

21.3 Where a Party is a Processor, the only processing that it is authorised to do is listed in Schedule 31 (*Processing Personal Data*) by the Controller and may not be determined by the Processor. The term "processing" and any associated terms are to be read in accordance with Article 4 of the UK GDPR and EU GDPR (as applicable).

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 21.4 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.
- 21.5 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:
- (a) a systematic description of the envisaged processing operations and the purpose of the processing;
 - (b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;
 - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
 - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
- 21.6 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Contract:
- (a) process that Personal Data only in accordance with Schedule 31 (*Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Authority before processing the Personal Data unless prohibited by Law;
 - (b) ensure that it has in place Protective Measures which are appropriate to protect against a Data Loss Event, including in the case of the Supplier the measures set out in Clause 18 (*Authority Data and Security Requirements*), which the Controller may reasonably reject. In the event of the Controller reasonably rejecting Protective Measures put in place by the Processor, the Processor must propose alternative Protective Measures to the satisfaction of the Controller. Failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures. Protective Measures must take account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Data Loss Event;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
 - (c) ensure that:
 - (i) the Processor Personnel do not process Personal Data except in accordance with this Contract (and in particular Schedule 31 (*Processing Personal Data*));

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (A) are aware of and comply with the Processor's duties under this Clause 21, Clauses 19 (*Confidentiality*) and 18 (*Authority Data and Security Requirements*);
 - (B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
 - (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by this Contract; and
 - (D) have undergone adequate training in the use, care, protection and handling of Personal Data;
- (d) not transfer such Personal Data outside of the UK and/or the EEA unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
 - (i) the destination country has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR (or section 74A of DPA 2018) and/or the transfer is in accordance with Article 45 of the EU GDPR (where applicable); or
 - (ii) the Controller and/or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75 and/or Article 46 of the EU GDPR (where applicable)) as determined by the Controller which could include relevant parties entering into:
 - (A) where the transfer is subject to UK GDPR:
 - (a) the UK International Data Transfer Agreement as published by the Information Commissioner's Office under section 119A(1) of the DPA 2018 from time to time; or
 - (b) the European Commission's Standard Contractual Clauses per decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time ("**EU SCCs**"), together with the UK International Data Transfer Agreement Addendum to the EU SCCs

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

(the “**Addendum**”) as published by the Information Commissioner's Office from time to time; and/or

(B) where the transfer is subject to EU GDPR, the EU SCCs,

as well as any additional measures determined by the Controller being implemented by the importing party;

(iii) the Data Subject has enforceable rights and effective legal remedies;

(iv) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

(v) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data; and

(e) (e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

21.7 Subject to Clause 21.8, the Processor shall notify the Controller immediately if it:

- (a) receives a Data Subject Request (or purported Data Subject Request);
- (b) receives a request to rectify, block or erase any Personal Data;
- (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
- (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;
- (e) receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
- (f) becomes aware of a Data Loss Event.

21.8 The Processor's obligation to notify under Clause 21.7 shall include the provision of further information to the Controller in phases, as details become available.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 21.9 Taking into account the nature of the processing, the Processor shall provide the Controller with reasonable assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause 21.7 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:
- (a) the Controller with full details and copies of the complaint, communication or request;
 - (b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;
 - (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
 - (d) assistance as requested by the Controller following any Data Loss Event; and/or
 - (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office or any other regulatory authority, or any consultation by the Controller with the Information Commissioner's Office or any other regulatory authority.
- 21.10 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Clause 21. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
- (a) the Controller determines that the processing is not occasional;
 - (b) the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
 - (c) the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.
- 21.11 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
- 21.12 The Parties shall designate its own Data Protection Officer if required by the Data Protection Legislation.
- 21.13 Before allowing any Sub-processor to process any Personal Data related to this Contract, the Processor must:
- (a) notify the Controller in writing of the intended Sub-processor and processing;
 - (b) obtain the written consent of the Controller;

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this Clause 21 such that they apply to the Sub-processor; and
- (d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

21.14 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.

21.15 Not used.

21.16 The Parties agree to take account of any guidance issued by the Information Commissioner's Office or any other relevant regulatory authority. The Authority may on not less than 30 Working Days' notice to the Supplier amend this Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office or any other relevant regulatory authority.

Where the Parties are Joint Controllers of Personal Data

21.17 In the event that the Parties are Joint Controllers in respect of Personal Data under this Contract, the Parties shall implement Clauses that are necessary to comply with Article 26 of the UK GDPR based on the terms set out in Annex 1 to Schedule 31 (*Processing Personal Data*).

Where the Parties are Independent Controllers of Personal Data

21.18 With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party shall comply with the provisions of Annex 4 of Schedule 31 (*Processing Personal Data*).

21.19 Not used.

21.20 Not used.

21.21 Not used.

21.22 Not used.

21.23 Not used

21.24 Not used

21.25 Not used

21.26 Not used

21.27 Not used

21.28 Not used

21.29 Notwithstanding the general application of Clauses 21.3 to 21.16 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with Clause 21.18.

Standard Contractual Clauses

21.30 It is noted that on 28 June 2021 the European Commission made an implementing decision pursuant to Article 45 of the EU GDPR on the adequate protection of personal data by the United Kingdom which contains carve-outs for certain transfers outside of the EU to the UK of certain types of Personal Data (the "**UK Adequacy Decision**"). If any transfer of Personal Data which is subject to EU GDPR pursuant to this Contract is not covered by the UK Adequacy Decision or at any time during the term of the Contract the UK Adequacy Decision is:

- (a) withdrawn, invalidated, overruled or otherwise ceases to have effect, or
- (b) amended in such a way as to affect the transfers of Personal Data outside of the EU which are contemplated under this Contract,

Clauses 21.31 to 21.32 below shall apply.

21.31 The Parties agree:

- (a) that without any further action being required they have entered into the Standard Contractual Clauses in the European Commission's decision 2021/914/EU in respect of data transfers by the Supplier outside of the EU to the UK;
- (b) that, where no other appropriate safeguard or exemption applies, that the Personal Data subject to this Contract (and to which Chapter V of the EU GDPR applies) will be transferred in accordance with those Standard Contractual Clauses as of the date the Parties entered into those Standard Contractual Clauses;
- (c) to use best endeavours to complete the annexes to the Standard Contractual Clauses promptly and at their own cost for the purpose of giving full effect to them; and
- (d) that if there is any conflict between this Contract and the Standard Contractual Clauses the terms of the Standard Contractual Clauses shall apply.

21.32 In the event that the European Commission updates, amends, substitutes, adopts or publishes new Standard Contractual Clauses from time to time, the Parties agree:

- (a) that the most up to date Standard Contractual Clauses from time to time shall be automatically incorporated in place of those in use at the time of such update, amendment, substitution, adoption or publication and that such incorporation is not a Change;

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) that where no other appropriate safeguard or exemption applies, that the Personal Data subject to this Contract (and to which Chapter V of the EU GDPR applies) will be transferred in accordance with the relevant form of the most up to date Standard Contractual Clauses as of the date the European Commission decision regarding such new Standard Contractual Clauses becomes effective;
- (c) to use best endeavours to complete any part of the most up to date Standard Contractual Clauses that a Party must complete promptly and at their own cost for the purpose of giving full effect to them; and
- (d) that if there is any conflict between this Contract and the most up to date Standard Contractual Clauses the terms of the most up to date Standard Contractual Clauses shall apply.

22 PUBLICITY AND BRANDING

22.1 The Supplier shall not:

- (a) make any press announcements or publicise this Contract or its contents in any way; or
- (b) use the Authority's name or brand in any promotion or marketing or announcement of orders;

without the prior written consent of the Authority, which shall not be unreasonably withheld or delayed.

22.2 Each Party acknowledges to the other that nothing in this Contract either expressly or by implication constitutes an endorsement of any products or services of the other Party (including the Services, the Supplier System and the Authority System) and each Party agrees not to conduct itself in such a way as to imply or express any such approval or endorsement.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SECTION G – LIABILITY, INDEMNITIES AND INSURANCE

23 LIMITATIONS ON LIABILITY

Unlimited liability

23.1 Neither Party limits its liability for:

- (a) death or personal injury caused by its negligence, or that of its employees, agents or sub-contractors (as applicable);
- (b) fraud or fraudulent misrepresentation by it or its employees;
- (c) breach of any obligation as to title implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Goods and Services Act 1982; or
- (d) any liability to the extent it cannot be limited or excluded by Law.

23.2 The Supplier's liability in respect of the indemnities in Clause 10.5 (*VAT*), Clause 14.7 (*Employment Indemnity*), Clause 14.8 (*Income Tax and National Insurance Contributions*), Clause 17 (*IPRs Indemnity*), Schedule 28 (*Staff Transfer*) and the Annexes to Schedule 28 (*Staff Transfer*) shall be unlimited.

23.3 The Authority's liability in respect of the indemnities in Clause 14.7 (*Employment Indemnity*), Schedule 28 (*Staff Transfer*) and the Annexes to Schedule 28 (*Staff Transfer*) shall be unlimited.

Financial and other limits

23.4 Subject to Clauses 23.1 and 23.2 (*Unlimited Liability*) and Clauses 23.7 (*Consequential losses*):

- (a) the Supplier's aggregate liability in respect of loss of or damage to the Authority Premises or other property or assets of the Authority and/or a Service Recipient (including technical infrastructure, assets or equipment but excluding any loss or damage to the Authority's Data or any other data) that is caused by Defaults of the Supplier occurring in each and any Contract Year shall in no event [REDACTED]
- (b) the Supplier's aggregate liability in respect of loss or damage to Authority Data and the indemnity at Clause 21.1 in each and any Contract Year shall in no event [REDACTED]
- (c) the Supplier's aggregate liability:
 - (i) in respect of all Service Credits incurred in any Service Period shall be subject to the Service Credit Cap; and
 - (ii) in respect of all Compensation for Unacceptable KPI Failure incurred in any consecutive period of 12 months shall in no

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

event exceed an amount equal to [REDACTED] of the Service Charges applicable during that 12 month period; and

- (d) the Supplier's aggregate liability in respect of all other Losses incurred by the Authority and/or a Service Recipient under or in connection with this Contract as a result of Defaults by the Supplier, including the Supplier's aggregate liability in respect of the indemnities at Clauses 5.3(b), 9.7(f) and 9.7(g) shall in no event exceed:
- (i) in relation to Defaults occurring in the first Contract Year, an amount equal to [REDACTED] of the Estimated Year 1 Charges;
 - (ii) in relation to Defaults occurring during any subsequent Contract Year, an amount equal to [REDACTED] of the Charges paid and/or due to be paid to the Supplier under this Contract in the Contract Year immediately preceding the occurrence of the Default; and
 - (iii) in relation to Defaults occurring after the end of the Term, an amount equal to [REDACTED] of the Charges paid and/or due to be paid to the Supplier in the 12 month period immediately prior to the last day of the Term,

provided that where any Losses referred to this Clause 23.4(d) have been incurred by the Authority and/or a Service Recipient as a result of the Supplier's abandonment of this Contract or the Supplier's wilful breach of a fundamental term of this Contract or wilful repudiatory breach of this Contract or the Supplier's aggregate liability in respect of the indemnity at Clause 3.8, the references in such Clause to [REDACTED] shall be deemed to be references to [REDACTED]

23.5 Deductions from Charges shall not be taken into consideration when calculating the Supplier's liability under Clause 23.4(c).

23.6 Subject to Clauses 23.1 and 23.3 (*Unlimited Liability*) and Clause 23.7 (*Consequential Losses*) and without prejudice to the Authority's obligation to pay the Charges as and when they fall due for payment:

- (a) the Authority's and/or a Service Recipient total aggregate liability in respect of all Losses incurred by the Supplier under or in connection with this Contract as a result of early termination of this Contract by the Authority pursuant to Clause 31.1(a) (*Termination by the Authority*),), 31.1A (*Partial Termination for Convenience*) or by the Supplier pursuant to Clause 31.3(a) (*Termination by the Supplier*) shall in no event exceed the following amounts:
- (i) in relation to the Unrecovered Payment, the amount set out in Paragraph 4 of Schedule 16 (*Payments on Termination*);
 - (ii) in relation to the Breakage Costs Payment, the amount set out in Paragraph 3.2 of Schedule 16 (*Payments on Termination*); and

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (iii) in relation to the Compensation Payment, the amount set out in Paragraph 6 of Schedule 16 (*Payments on Termination*); and
- (b) the Authority's and/or a Service Recipient's aggregate liability in respect of all Losses incurred by the Supplier under or in connection with this Contract as a result of Defaults of the Authority shall in no event exceed:
 - (i) in relation to Defaults occurring in the first Contract Year, an amount equal to the Estimated Year 1 Charges;
 - (ii) in relation to Defaults occurring during any subsequent Contract Year, an amount equal to the total Charges paid and/or due to be paid under this Contract in the Contract Year immediately preceding the occurrence of the Default; and
 - (iii) in relation to Defaults occurring after the end of the Term, an amount equal to the total Charges paid and/or due to be paid to the Supplier in the 12 month period immediately prior to the last day of the Term.

Consequential Losses

23.7 Subject to Clauses 23.1, 23.2 and 23.3 (*Unlimited Liability*) and Clause 23.8, neither Party shall be liable to the other Party for:

- (a) any indirect, special or consequential Loss; and/or
- (b) any loss of profits, turnover, business opportunities or damage to goodwill (in each case whether direct or indirect).

23.8 Notwithstanding Clause 23.7 but subject to Clause 23.4, the Supplier acknowledges that the Authority may, amongst other things, recover from the Supplier the following Losses incurred by the Authority and/or a Service Recipient to the extent that they arise as a result of a Default by the Supplier:

- (a) any additional operational and/or administrative costs and expenses incurred by the Authority, including costs relating to time spent by or on behalf of the Authority in dealing with the consequences of the Default;
- (b) any wasted expenditure or charges;
- (c) the additional cost of procuring Replacement Services for the remainder of the Term and/or replacement Deliverables, which shall include any incremental costs associated with such Replacement Services and/or replacement Deliverables above those which would have been payable under this Contract;
- (d) any compensation or interest paid to a third party by the Authority and/or a Service Recipient;

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (e) any fine or penalty incurred by the Authority pursuant to Law and any costs incurred by the Authority and/or a Service Recipient in defending any proceedings which result in such fine or penalty; and
- (f) any anticipated savings identified in Schedule 20 (*Anticipated Savings*).

Conduct of indemnity claims

23.9 Where under this Contract one Party indemnifies the other Party, the Parties shall comply with the provisions of Schedule 27 (*Conduct of Claims*) in relation to the conduct of claims made by a third person against the Party having (or claiming to have) the benefit of the indemnity.

Mitigation

23.10 Each Party shall use all reasonable endeavours to mitigate any loss or damage suffered arising out of or in connection with this Contract, including any Losses for which the relevant Party is entitled to bring a claim against the other Party pursuant to the indemnities in this Contract.

24 INSURANCE

24.1 The Supplier shall comply with the provisions of Schedule 6 (*Insurance Requirements*) in relation to obtaining and maintaining insurance.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SECTION H – REMEDIES AND RELIEF**25 RECTIFICATION PLAN PROCESS**

25.1 In the event that:

- (a) there is, or is reasonably likely to be, a Delay; and/or
- (b) in any Service Period there has been:
 - (i) a Material KPI Failure; and/or
 - (ii) a Material PI Failure; and/or
- (c) the Supplier commits a material Default that is capable of remedy,

(each a “**Notifiable Default**”), the Supplier shall notify the Authority of the Notifiable Default as soon as practicable but in any event within 3 Working Days of becoming aware of the Notifiable Default, detailing the actual or anticipated effect of the Notifiable Default and, unless the Notifiable Default also constitutes a Rectification Plan Failure or other Supplier Termination Event, the Authority may not terminate this Contract in whole or in part on the grounds of the Notifiable Default without first following the Rectification Plan Process.

Notification

25.2 If:

- (a) the Supplier notifies the Authority pursuant to Clause 25.1 that a Notifiable Default has occurred; or
- (b) the Authority notifies the Supplier that it considers that a Notifiable Default has occurred (setting out sufficient detail so that it is reasonably clear what the Supplier has to rectify),

then, unless the Notifiable Default also constitutes a Supplier Termination Event and the Authority serves a Termination Notice, the Supplier shall comply with the Rectification Plan Process.

25.3 The “**Rectification Plan Process**” shall be as set out in Clauses 25.4 (*Submission of the draft Rectification Plan*) to 25.9 (*Agreement of the Rectification Plan*).

Submission of the draft Rectification Plan

25.4 The Supplier shall submit a draft Rectification Plan to the Authority for it to review as soon as possible and in any event within 10 Working Days (or such other period as may be agreed between the Parties) after the original notification pursuant to Clause 25.2 (*Notification*). The Supplier shall submit a draft Rectification Plan even if the Supplier disputes that it is responsible for the Notifiable Default.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

25.5 The draft Rectification Plan shall set out:

- (a) full details of the Notifiable Default that has occurred, including a root cause analysis;
- (b) the actual or anticipated effect of the Notifiable Default; and
- (c) the steps which the Supplier proposes to take to rectify the Notifiable Default (if applicable) and to prevent such Notifiable Default from recurring, including timescales for such steps and for the rectification of the Notifiable Default (where applicable).

25.6 The Supplier shall promptly provide to the Authority any further documentation that the Authority reasonably requires to assess the Supplier's root cause analysis. If the Parties do not agree on the root cause set out in the draft Rectification Plan, either Party may refer the matter to be determined by an expert in accordance with Paragraph 6 of Schedule 23 (*Dispute Resolution Procedure*).

Agreement of the Rectification Plan

25.7 The Authority may reject the draft Rectification Plan by notice to the Supplier if, acting reasonably, it considers that the draft Rectification Plan is inadequate, for example because the draft Rectification Plan:

- (a) is insufficiently detailed to be capable of proper evaluation;
- (b) will take too long to complete;
- (c) will not prevent reoccurrence of the Notifiable Default; and/or
- (d) will rectify the Notifiable Default but in a manner which is unacceptable to the Authority.

25.8 The Authority shall notify the Supplier whether it consents to the draft Rectification Plan as soon as reasonably practicable. If the Authority rejects the draft Rectification Plan, the Authority shall give reasons for its decision and the Supplier shall take the reasons into account in the preparation of a revised Rectification Plan. The Supplier shall submit the revised draft of the Rectification Plan to the Authority for review within 5 Working Days (or such other period as agreed between the Parties) of the Authority's notice rejecting the first draft.

25.9 If the Authority consents to the Rectification Plan:

- (a) the Supplier shall immediately start work on the actions set out in the Rectification Plan; and
- (b) the Authority may no longer terminate this Contract in whole or in part on the grounds of the relevant Notifiable Default;

save in the event of a Rectification Plan Failure or other Supplier Termination Event.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

26 DELAY PAYMENTS

- 26.1 If a Key Milestone has not been Achieved by its relevant Milestone Date, the provisions of Paragraph 1 of Part C of Schedule 15 (*Charges and Invoicing*) shall apply in relation to the payment of Delay Payments.
- 26.2 Delay Payments shall be the Authority's exclusive financial remedy for the Supplier's failure to Achieve a Key Milestone by its Milestone Date except where:
- (a) the Authority is entitled to or does terminate this Contract pursuant to Clause 31.1(b) (*Termination by the Authority*); or
 - (b) the Delay exceeds the Delay Deduction Period.

27 REMEDIAL ADVISER

- 27.1 If:
- (a) any of the Intervention Trigger Events occur; or
 - (b) the Authority reasonably believes that any of the Intervention Trigger Events are likely to occur,
- (each an "**Intervention Cause**"), the Authority may give notice to the Supplier (an "**Intervention Notice**") giving reasonable details of the Intervention Cause and requiring:
- (i) a meeting between the Authority Representative and the Supplier Representative to discuss the Intervention Cause; and/or
 - (ii) the appointment as soon as practicable by the Supplier of a Remedial Adviser, as further described in this Clause 27.

For the avoidance of doubt, if the Intervention Cause is also a Supplier Termination Event, the Authority has no obligation to exercise its rights under this Clause 27.1 prior to or instead of exercising its right to terminate this Contract.

- 27.2 If the Authority gives notice that it requires the appointment of a Remedial Adviser:
- (a) the Remedial Adviser shall be:
 - (i) a person selected by the Supplier and approved by the Authority; or
 - (ii) if none of the persons selected by the Supplier have been approved by the Authority (or no person has been selected by the Supplier) within 10 Working Days following the date on which the Intervention Notice is given, a person identified by the Authority;

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) the terms of engagement and start date agreed with the Remedial Adviser must be approved by the Authority; and
- (c) any right of the Authority to terminate this Contract pursuant to Clause 31.1(b) (*Termination by the Authority*) for the occurrence of that Intervention Cause shall be suspended for 60 Working Days from (and including) the date of the Intervention Notice (or such other period as may be agreed between the Parties)(the “**Intervention Period**”).

27.3 The Remedial Adviser’s overall objective shall be to mitigate the effects of, and (to the extent capable of being remedied) to remedy, the Intervention Cause and to avoid the occurrence of similar circumstances in the future. In furtherance of this objective (but without diminishing the Supplier’s responsibilities under this Contract), the Parties agree that the Remedial Adviser may undertake any one or more of the following actions:

- (a) observe the conduct of and work alongside the Supplier Personnel to the extent that the Remedial Adviser considers reasonable and proportionate having regard to the Intervention Cause;
- (b) gather any information the Remedial Adviser considers relevant in the furtherance of its objective;
- (c) write reports and provide information to the Authority in connection with the steps being taken by the Supplier to remedy the Intervention Cause;
- (d) make recommendations to the Authority and/or the Supplier as to how the Intervention Cause might be mitigated or avoided in the future; and/or
- (e) take any other steps that the Authority and/or the Remedial Adviser reasonably considers necessary or expedient in order to mitigate or rectify the Intervention Cause.

27.4 The Supplier shall:

- (a) work alongside, provide information to, co-operate in good faith with and adopt any reasonable methodology in providing the Services recommended by the Remedial Adviser;
- (b) ensure that the Remedial Adviser has all the access it may require in order to carry out its objective, including access to the Assets;
- (c) submit to such monitoring as the Authority and/or the Remedial Adviser considers reasonable and proportionate in respect of the Intervention Cause;
- (d) implement any reasonable recommendations made by the Remedial Adviser that have been approved by the Authority within the timescales given by the Remedial Adviser; and

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (e) not terminate the appointment of the Remedial Adviser prior to the end of the Intervention Period without the prior consent of the Authority (such consent not to be unreasonably withheld).

27.5 The Supplier shall be responsible for:

- (a) the costs of appointing, and the fees charged by, the Remedial Adviser; and
- (b) its own costs in connection with any action required by the Authority and/or the Remedial Adviser pursuant to this Clause 27.

27.6 If:

- (a) the Supplier:
 - (i) fails to perform any of the steps required by the Authority in an Intervention Notice; and/or
 - (ii) is in Default of any of its obligations under Clause 27.4; and/or
- (b) the relevant Intervention Trigger Event is not rectified by the end of the Intervention Period,

(each a “**Remedial Adviser Failure**”), the Authority shall be entitled to terminate this Contract pursuant to Clause 31.1(b) (*Termination by the Authority*).

28 STEP-IN RIGHTS

28.1 On the occurrence of a Step-In Trigger Event, the Authority may serve notice on the Supplier (a “**Step-In Notice**”) that it will be taking action under this Clause 28 (*Step-in Rights*), either itself or with the assistance of a third party (provided that the Supplier may require any third parties to comply with a confidentiality undertaking equivalent to Clause 19 (*Confidentiality*)). The Step-In Notice shall set out the following:

- (a) the action the Authority wishes to take and in particular the Services that it wishes to control (the “**Required Action**”);
- (b) the Step-In Trigger Event that has occurred and whether the Authority believes that the Required Action is due to the Supplier's Default;
- (c) the date on which it wishes to commence the Required Action;
- (d) the time period which it believes will be necessary for the Required Action;
- (e) whether the Authority will require access to the Supplier's premises and/or the Sites; and
- (f) to the extent practicable, the impact that the Authority anticipates the Required Action will have on the Supplier's obligations to provide the Services during the period that the Required Action is being taken.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

28.2 Following service of a Step-In Notice, the Authority shall:

- (a) take the Required Action set out in the Step-In Notice and any consequential additional action as it reasonably believes is necessary to achieve the Required Action;
- (b) keep records of the Required Action taken and provide information about the Required Action to the Supplier;
- (c) co-operate wherever reasonable with the Supplier in order to enable the Supplier to continue to provide the Services in relation to which the Authority is not assuming control; and
- (d) act reasonably in mitigating the cost that the Supplier will incur as a result of the exercise of the Authority's rights under this Clause 28.

28.3 For so long as and to the extent that the Required Action is continuing, then:

- (a) the Supplier shall not be obliged to provide the Services to the extent that they are the subject of the Required Action;
- (b) no Deductions shall be applicable in relation to Charges in respect of Services that are the subject of the Required Action and the provisions of Clause 28.4 shall apply to Deductions from Charges in respect of other Services; and
- (c) the Authority shall pay to the Supplier the Charges after subtracting any applicable Deductions and the Authority's costs of taking the Required Action.

28.4 If the Supplier demonstrates to the reasonable satisfaction of the Authority that the Required Action has resulted in:

- (a) the degradation of any Services not subject to the Required Action;
or
- (b) the non-Achievement of a Milestone,

beyond that which would have been the case had the Authority not taken the Required Action, then the Supplier shall be entitled to an agreed adjustment of the Charges.

28.5 Before ceasing to exercise its step in rights under this Clause 28 the Authority shall deliver a written notice to the Supplier (a "**Step-Out Notice**"), specifying:

- (a) the Required Action it has actually taken; and
- (b) the date on which the Authority plans to end the Required Action (the "**Step-Out Date**") subject to the Authority being satisfied with the Supplier's ability to resume the provision of the Services and the Supplier's plan developed in accordance with Clause 28.6.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 28.6 The Supplier shall, following receipt of a Step-Out Notice and not less than 20 Working Days prior to the Step-Out Date, develop for the Authority's approval a draft plan (a "**Step-Out Plan**") relating to the resumption by the Supplier of the Services, including any action the Supplier proposes to take to ensure that the affected Services satisfy the requirements of this Contract.
- 28.7 If the Authority does not approve the draft Step-Out Plan, the Authority shall inform the Supplier of its reasons for not approving it. The Supplier shall then revise the draft Step-Out Plan taking those reasons into account and shall re-submit the revised plan to the Authority for the Authority's approval. The Authority shall not withhold or delay its approval of the draft Step-Out Plan unnecessarily.
- 28.8 The Supplier shall bear its own costs in connection with any step-in by the Authority under this Clause 28, provided that the Authority shall reimburse the Supplier's reasonable additional expenses incurred directly as a result of any step-in action taken by the Authority under:
- (a) limbs (c) or (d) of the definition of a Step-In Trigger Event; or
 - (b) limbs (e) and (f) of the definition of a Step-in Trigger Event (insofar as the primary cause of the Authority serving the Step-In Notice is identified as not being the result of the Supplier's Default).

29 AUTHORITY CAUSE

- 29.1 Notwithstanding any other provision of this Contract, if the Supplier has failed to:

- (a) Achieve a Milestone by its Milestone Date;
- (b) provide the Operational Services in accordance with the Target Performance Levels; and/or
- (c) comply with its obligations under this Contract,

(each a "**Supplier Non-Performance**"),

and can demonstrate that the Supplier Non-Performance would not have occurred but for an Authority Cause, then (subject to the Supplier fulfilling its obligations in this Clause 29):

- (i) the Supplier shall not be treated as being in breach of this Contract to the extent the Supplier can demonstrate that the Supplier Non-Performance was caused by the Authority Cause;
- (ii) the Authority shall not be entitled to exercise any rights that may arise as a result of that Supplier Non-Performance:
 - (A) to terminate this Contract pursuant to Clause 31.1(b) (*Termination by the Authority*); or

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (B) to take action pursuant to Clauses 27 (*Remedial Adviser*) or 28 (*Step-In*);
- (iii) where the Supplier Non-Performance constitutes the failure to Achieve a Milestone by its Milestone Date:
 - (A) the Milestone Date shall be postponed by a period equal to the period of Delay that the Supplier can demonstrate was caused by the Authority Cause;
 - (B) if the Authority, acting reasonably, considers it appropriate, the Implementation Plan shall be amended to reflect any consequential revisions required to subsequent Milestone Dates resulting from the Authority Cause;
 - (C) if the Milestone is a Key Milestone, the Supplier shall have no liability to pay any Delay Payments associated with the Key Milestone to the extent that the Supplier can demonstrate that such failure was caused by the Authority Cause; and
 - (D) the Supplier shall be entitled to claim compensation subject to and in accordance with the principles set out in Paragraph 2 of Part C of Schedule 15 (*Charges and Invoicing*); and/or
- (iv) where the Supplier Non-Performance constitutes a Performance Failure:
 - (A) the Supplier shall not be liable to accrue Service Credits;
 - (B) the Authority shall not be entitled to withhold any of the Service Charges pursuant to Clause 7.2(d)(ii) (*Performance Failures*);
 - (C) the Authority shall not be entitled to withhold and retain any Compensation for Unacceptable KPI Failure pursuant to Clause 7.4(a) (*Unacceptable KPI Failure*); and
 - (D) the Supplier shall be entitled to invoice for the Service Charges for the relevant Operational Services affected by the Authority Cause,

in each case, to the extent that the Supplier can demonstrate that the Performance Failure was caused by the Authority Cause.

29.2 In order to claim any of the rights and/or relief referred to in Clause 29.1, the Supplier shall as soon as reasonably practicable (and in any event within 10

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Working Days) after becoming aware that an Authority Cause has caused, or is reasonably likely to cause, a Supplier Non-Performance, give the Authority notice (a “**Relief Notice**”) setting out details of:

- (a) the Supplier Non-Performance;
- (b) the Authority Cause and its effect, or likely effect, on the Supplier’s ability to meet its obligations under this Contract;
- (c) any steps which the Authority can take to eliminate or mitigate the consequences and impact of such Authority Cause; and
- (d) the relief and/or compensation claimed by the Supplier.

29.3 Following the receipt of a Relief Notice, the Authority shall as soon as reasonably practicable consider the nature of the Supplier Non-Performance and the alleged Authority Cause and whether it agrees with the Supplier’s assessment set out in the Relief Notice as to the effect of the relevant Authority Cause and its entitlement to relief and/or compensation, consulting with the Supplier where necessary.

29.4 The Supplier shall use all reasonable endeavours to eliminate or mitigate the consequences and impact of an Authority Cause, including any Losses that the Supplier may incur and the duration and consequences of any Delay or anticipated Delay.

29.5 Without prejudice to Clause 5.9 (*Continuing obligation to provide the Services*), if a Dispute arises as to:

- (a) whether a Supplier Non-Performance would not have occurred but for an Authority Cause; and/or
- (b) the nature and/or extent of the relief and/or compensation claimed by the Supplier,

either Party may refer the Dispute to the Dispute Resolution Procedure. Pending the resolution of the Dispute, both Parties shall continue to resolve the causes of, and mitigate the effects of, the Supplier Non-Performance.

29.6 Any Change that is required to the Implementation Plan or to the Charges pursuant to this Clause 29 shall be implemented in accordance with the Change Control Procedure.

30 FORCE MAJEURE

30.1 Subject to the remaining provisions of this Clause 30 (and, in relation to the Supplier, subject to its compliance with its obligations in Schedule 26 (*Service Continuity Plan and Corporate Resolution Planning*)), a Party may claim relief under this Clause 30 from liability for failure to meet its obligations under this Contract for as long as and only to the extent that the performance of those obligations is directly affected by a Force Majeure Event. Any failure or delay by the Supplier in performing its obligations under this Contract which results from

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

a failure or delay by an agent, Sub-contractor or supplier shall be regarded as due to a Force Majeure Event only if that agent, Sub-contractor or supplier is itself impeded by a Force Majeure Event from complying with an obligation to the Supplier.

- 30.2 The Affected Party shall as soon as reasonably practicable issue a Force Majeure Notice, which shall include details of the Force Majeure Event, its effect on the obligations of the Affected Party and any action the Affected Party proposes to take to mitigate its effect.
- 30.3 If the Supplier is the Affected Party, it shall not be entitled to claim relief under this Clause 30 to the extent that consequences of the relevant Force Majeure Event:
- (a) are capable of being mitigated, but the Supplier has failed to do so;
 - (b) should have been foreseen and prevented or avoided by a prudent provider of services similar to the Services, operating to the standards required by this Contract; or
 - (c) are the result of the Supplier's failure to comply with its Service Continuity Plan (except to the extent that such failure is also due to a Force Majeure Event that affects the execution of the Service Continuity Plan).
- 30.4 Subject to Clause 30.5, as soon as practicable after the Affected Party issues the Force Majeure Notice, and at regular intervals thereafter, the Parties shall consult in good faith and use reasonable endeavours to agree any steps to be taken and an appropriate timetable in which those steps should be taken, to enable continued provision of the Services affected by the Force Majeure Event.
- 30.5 The Parties shall at all times following the occurrence of a Force Majeure Event and during its subsistence use their respective reasonable endeavours to prevent and mitigate the effects of the Force Majeure Event. Where the Supplier is the Affected Party, it shall take all steps in accordance with Good Industry Practice to overcome or minimise the consequences of the Force Majeure Event.
- 30.6 Where, as a result of a Force Majeure Event:
- (a) an Affected Party fails to perform its obligations in accordance with this Contract, then during the continuance of the Force Majeure Event:
 - (i) the other Party shall not be entitled to exercise any rights to terminate this Contract in whole or in part as a result of such failure other than pursuant to Clause 31.1(c) (*Termination by the Authority*) or Clause 31.3(b) (*Termination by the Supplier*); and
 - (ii) neither Party shall be liable for any Default arising as a result of such failure;

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) the Supplier fails to perform its obligations in accordance with this Contract:
 - (i) the Authority shall not be entitled:
 - (A) during the continuance of the Force Majeure Event to exercise its rights under Clause 27 (*Remedial Adviser*) and/or Clause 28 (*Step-in Rights*) as a result of such failure;
 - (B) to receive Delay Payments pursuant to Clause 26 (*Delay Payments*) to the extent that the Achievement of any Milestone is affected by the Force Majeure Event; and
 - (C) to receive Service Credits, to withhold any of the Service Charges pursuant to Clause 7.2(d)(ii) (*Performance Failures*) or withhold and retain any of the Service Charges as compensation pursuant to Clause 7.4(a) (*Unacceptable KPI Failure*) to the extent that a Performance Failure has been caused by the Force Majeure Event; and
 - (ii) the Supplier shall be entitled to receive payment of the Charges (or a proportional payment of them) only to the extent that the Services (or part of the Services) continue to be performed in accordance with the terms of this Contract during the occurrence of the Force Majeure Event.
- 30.7 The Affected Party shall notify the other Party as soon as practicable after the Force Majeure Event ceases or no longer causes the Affected Party to be unable to comply with its obligations under this Contract.
- 30.8 Relief from liability for the Affected Party under this Clause 30 shall end as soon as the Force Majeure Event no longer causes the Affected Party to be unable to comply with its obligations under this Contract and shall not be dependent on the serving of notice under Clause 30.7.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SECTION I – TERMINATION AND EXIT MANAGEMENT**31 TERMINATION RIGHTS****Termination by the Authority**

31.1 The Authority may terminate this Contract by issuing a Termination Notice to the Supplier:

- (a) for convenience at any time;
- (b) if a Supplier Termination Event occurs;
- (c) if a Force Majeure Event endures for a continuous period of more than ninety (90) days; or
- (d) if the Contract has been substantially amended to the extent that the Public Contracts Regulations 2015 require a new procurement procedure,

and this Contract shall terminate on the date specified in the Termination Notice.

Partial Termination

31.1A Without prejudice to any other rights or remedies of the Authority howsoever arising, the Authority may partially terminate for convenience any part of the Services by complying with the provisions of Paragraph 11 (Partial Termination of Services) of Schedule 25 (Exit Management).

31.2 Where the Authority:

- (a) is terminating this Contract under Clause 31.1(b) due to the occurrence of either limb (b),(h) and/or (i) of the definition of Supplier Termination Event, it may rely on a single material Default or on a number of Defaults or repeated Defaults (whether of the same or different obligations and regardless of whether such Defaults are cured) which taken together constitute a material Default; and/or
- (b) has the right to terminate this Contract under Clause 31.1(b) or Clause 31.1(c), it may, prior to or instead of terminating the whole of this Contract, serve a Termination Notice requiring the partial termination of this Contract to the extent that it relates to any part of the Services which are materially affected by the relevant circumstances.

Termination by the Supplier

31.3 The Supplier may, by issuing a Termination Notice to the Authority, terminate:

- (a) this Contract if the Authority fails to pay an undisputed sum due to the Supplier under this Contract which in aggregate [REDACTED] and such amount [REDACTED]

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

remains outstanding 40 Working Days after the receipt by the Authority of a notice of non-payment from the Supplier; or

- (b) any Services that are materially impacted by a Force Majeure Event that endures for a continuous period of more than ninety (90) days,

and this Contract or the relevant Services (as the case may be) shall then terminate on the date specified in the Termination Notice (which shall not be less than 20 Working Days from the date of the issue of the Termination Notice). If the operation of Clause 31.3(b) would result in a Partial Termination, the provisions of Clause 31.4 (*Partial Termination*) shall apply.

Partial Termination

- 31.4 If the Supplier notifies the Authority pursuant to Clause 31.3(b) (*Termination by the Supplier*) that it intends to terminate this Contract in part and the Authority, acting reasonably, believes that the effect of such Partial Termination is to render the remaining Services incapable of meeting a significant part of the Authority Requirements, then the Authority shall be entitled to terminate the remaining part of this Contract by serving a Termination Notice to the Supplier within 1 month of receiving the Supplier's Termination Notice. For the purpose of this Clause 31.4, in assessing the significance of any part of the Authority Requirements, regard shall be had not only to the proportion of that part to the Authority Requirements as a whole, but also to the importance of the relevant part to the Authority.
- 31.5 The Parties shall agree the effect of any Change necessitated by a Partial Termination in accordance with the Change Control Procedure, including the effect the Partial Termination may have on any other Services and the Charges, provided that:
- (a) the Supplier shall not be entitled to an increase in the Charges in respect of the Services that have not been terminated if the Partial Termination arises due to the occurrence of a Supplier Termination Event;
 - (b) any adjustment to the Charges (if any) shall be calculated in accordance with the Financial Model and must be reasonable; and
 - (c) the Supplier shall not be entitled to reject the Change.

32 CONSEQUENCES OF EXPIRY OR TERMINATION**General Provisions on Expiry or Termination**

- 32.1 The provisions of Clauses 5.8 (*Specially Written Software warranty*), 9.7(f) (*Indemnity against the recall of goods*), 10.4 and 10.5 (VAT), 10.6 and 10.7 (*Set-off and Withholding*), 12 (*Records, Reports, Audits and Open Book Data*), 14.7 (*Employment Indemnity*), 14.8 (*Income Tax and National Insurance Contributions*), 16 (*Intellectual Property Rights*), 17.1 (*IPRs Indemnity*), 19 (*Confidentiality*), 20 (*Transparency and Freedom of Information*), 21 (*Protection of Personal Data*), 23 (*Limitations on Liability*), 32 (*Consequences of Expiry or*

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Termination), 38 (*Severance*), 40 (*Entire Agreement*), 41 (*Third Party Rights*), 43 (*Disputes*) and 44 (*Governing Law and Jurisdiction*), and the provisions of Schedules 1 (*Definitions*), 15 (*Charges and Invoicing*), 16 (*Payments on Termination*), 19 (*Financial Reports and Audit Rights*), 23 (*Dispute Resolution Procedure*), 24 (*Reports and Records Provisions*), 25 (*Exit Management*), 28 (*Staff Transfer*), and 32 (*Intellectual Property Rights*), shall survive the termination or expiry of this Contract.

- 32.2 Accumulated rights of the Parties shall not be affected by termination or expiry of the Contract.

Exit Management

- 32.3 The Parties shall comply with the provisions of Schedule 25 (*Exit Management*) and any current Exit Plan in relation to orderly transition of the Services to the Authority or a Replacement Supplier.

Payments by the Authority

- 32.4 If this Contract is terminated by the Authority pursuant to Clauses 31.1(a) (*Termination by the Authority*) or by the Supplier pursuant to Clause 31.3(a) (*Termination by the Supplier*) or 34.4, the Authority shall pay the Supplier the following payments (which shall be the Supplier's sole remedy for the termination of this Contract):

- (a) the Termination Payment; and
- (b) the Compensation Payment, if either of the following periods is less than three hundred and sixty-five (365) days:
 - (i) the period from (but excluding) the date that the Termination Notice is given (or, where Paragraph 2.1(d) of Part D of Schedule 15 (*Charges and Invoicing*) applies, deemed given) by the Authority pursuant to Clause 31.1(a) (*Termination by the Authority*)) to (and including) the Termination Date; or
 - (ii) the period from (and including) the date of the non-payment by the Authority referred to in Clause 31.3(a) (*Termination by the Supplier*) to (and including) the Termination Date.

- 32.5 If this Contract is terminated (in part or in whole) by the Authority pursuant to Clauses 31.1(b), 31.1(c) and/or 31.2 (*Termination by the Authority*), 33.8(l)(ii) and/or 33.12(b) or the Term expires, the only payments that the Authority shall be required to make as a result of such termination (whether by way of compensation or otherwise) are:

- (a) payments in respect of any Assets or apportionments in accordance with Schedule 25 (*Exit Management*); and
- (b) payments in respect of unpaid Charges for Services received up until the Termination Date.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

32.6 The costs of termination incurred by the Parties shall lie where they fall if:

- (a) either Party terminates or partially terminates this Contract for a continuing Force Majeure Event pursuant to Clauses 31.1(c) or 31.2(b) (*Termination by the Authority*) or 31.3(b) (*Termination by the Supplier*); or
- (b) the Authority terminates this Contract under Clause 31.1(d) (*Termination by the Authority*).

Payments by the Supplier

32.7 In the event of termination or expiry of this Contract, the Supplier shall repay to the Authority all Charges it has been paid in advance in respect of Services not provided by the Supplier as at the date of expiry or termination.

32.8 If this Contract is terminated (in whole or in part) by the Authority pursuant to Clause 31.1(b) (*Termination by the Authority*) prior to Achievement of one or more CPP Milestones, the Authority may at any time on or within 12 months of the issue of the relevant Termination Notice by issue to the Supplier of written notice (a "**Milestone Adjustment Payment Notice**") require the Supplier to repay to the Authority an amount equal to the aggregate Milestone Adjustment Payment Amounts in respect of each CPP Milestone to which the Milestone Adjustment Payment Notice relates.

32.9 A Milestone Adjustment Payment Notice shall specify:

- (a) each CPP Milestone to which it relates;
- (b) in relation to each such CPP Milestone, each Deliverable relating to that CPP Milestone that the Authority wishes to retain, if any (each such Deliverable being a "**Retained Deliverable**"); and
- (c) those Retained Deliverables, if any, the Allowable Price for which the Authority considers should be subject to deduction of an adjusting payment on the grounds that they do not or will not perform in all material respects in accordance with their specification (such adjusting payment being an "**Allowable Price Adjustment**"),

and may form part of a Termination Notice.

32.10 The Supplier shall within 10 Working Days of receipt of a Milestone Adjustment Payment Notice, in each case as applicable:

- (a) notify the Authority whether it agrees that the Retained Deliverables which the Authority considers should be subject to an Allowable Price Adjustment as specified in the relevant Milestone Adjustment Payment Notice should be so subject; and
- (b) in relation to each such Retained Deliverable that the Supplier agrees should be subject to an Allowable Price Adjustment, notify the

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Authority of the Supplier's proposed amount of the Allowable Price Adjustment and the basis for its approval;

- (c) provide the Authority with its calculation of the Milestone Adjustment Payment Amount in respect of each CPP Milestone the subject of the relevant Milestone Adjustment Payment Notice using its proposed Allowable Price Adjustment, including details of:
 - (i) all relevant Milestone Payments; and
 - (ii) the Allowable Price of each Retained Deliverable; and
- (d) provide the Authority with such supporting information as the Authority may require.

32.11 If the Parties do not agree the calculation of a Milestone Adjustment Payment Amount within 20 Working Days of the Supplier's receipt of the relevant Milestone Adjustment Payment Notice, either Party may refer the Dispute to the Dispute Resolution Procedure.

32.12 If the Authority issues a Milestone Adjustment Payment Notice pursuant to Clause 32.8:

- (a) the Authority shall:
 - (i) securely destroy or return to the Supplier all Non-retained Deliverables that are in tangible form; and
 - (ii) ensure that all Non-retained Deliverables that are held in electronic, digital or other machine-readable form cease to be readily accessible (other than by the information technology staff of the Authority) from any computer, word processor, voicemail system or any other device containing such all Non-retained Deliverables,

in each case as soon as reasonably practicable after repayment of the aggregate Milestone Adjustment Payment Amounts repayable pursuant to that Milestone Adjustment Payment Notice; and

- (b) all licences granted by the Supplier pursuant to Schedule 32 (*Intellectual Property Rights*) in respect of Specially Written Software and Project Specific IPRs and any Supplier Non-COTS Software and/or Supplier Background IPRs shall terminate upon such repayment to the extent that they relate to the Non-retained Deliverables.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SECTION J – MISCELLANEOUS AND GOVERNING LAW**33 COMPLIANCE****Health and Safety**

33.1 The Supplier shall perform its obligations under this Contract (including those in relation to the Services) in accordance with:

- (a) all applicable Law regarding health and safety; and
- (b) the Health and Safety Policy whilst at the Authority Premises.

33.2 Each Party shall notify the other as soon as practicable of any health and safety incidents or material health and safety hazards at the Authority Premises of which it becomes aware and which relate to or arise in connection with the performance of this Contract. The Supplier shall instruct the Supplier Personnel to adopt any necessary associated safety measures in order to manage any such material health and safety hazards.

Employment Law

33.3 The Supplier must perform its obligations meeting the requirements of all applicable Law regarding employment.

Equality and Diversity

33.4 The Supplier shall:

- (a) perform its obligations under this Contract (including those in relation to the Services) in accordance with:
 - (i) all applicable equality Law (whether in relation to race, sex, gender reassignment, age, disability, sexual orientation, religion or belief, pregnancy, maternity or otherwise);
 - (ii) the Authority's equality and diversity policy as provided to the Supplier from time to time; and
 - (iii) any other requirements and instructions which the Authority reasonably imposes in connection with any equality obligations imposed on the Authority at any time under applicable equality Law; and
- (b) take all necessary steps, and inform the Authority of the steps taken, to prevent unlawful discrimination designated as such by any court or tribunal, or the Equality and Human Rights Commission or (any successor organisation).

Official Secrets Act and Finance Act

33.5 The Supplier shall comply with the provisions of:

- (a) the Official Secrets Acts 1911 to 1989; and

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) section 182 of the Finance Act 1989.

Conflicts of Interest**33.6 The Supplier:**

- (a) must take action to ensure that neither the Supplier nor the Supplier Personnel are placed in the position of an actual, potential or perceived Conflict of Interest.
- (b) must promptly notify and provide details to the Authority if an actual, potential or perceived Conflict of Interest happens or is expected to happen.

33.7 The Authority will consider whether there are any appropriate measures that can be put in place to remedy an actual, perceived or potential Conflict of Interest. If, in the reasonable opinion of the Authority, such measures do not or will not resolve an actual or potential Conflict of Interest, the Authority may terminate this Contract in accordance with Clause 31.1(b) immediately by giving notice in writing to the Supplier where there is or may be an actual or potential Conflict of Interest and Clauses 32.3, 32.5 and 32.7 to 32.12 shall apply.

Modern Slavery**33.8 The Supplier:**

- (a) shall not use, nor allow its sub-contractors to use forced, bonded or involuntary prison labour;
- (b) shall not require any Supplier Personnel or the personnel of any sub-contractors to lodge deposits or identity papers with their employer and shall be free to leave their employer after reasonable notice;
- (c) warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world;
- (d) warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offences anywhere around the world;
- (e) shall make reasonable enquires to ensure that its officers, employees and sub-contractors have not been convicted of slavery or human trafficking offences anywhere around the world;
- (f) shall have and maintain throughout the Term its own policies and procedures to ensure its compliance with the Modern Slavery Act 2015 and include in its contracts with its sub-contractors anti-slavery and human trafficking provisions;

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (g) shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under the Contract;
- (h) shall prepare and deliver to the Authority, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business;
- (i) shall not use, nor allow its employees or sub-contractors to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or sub-contractors;
- (j) shall not use or allow child or slave labour to be used by its sub-contractors;
- (k) shall report the discovery or suspicion of any slavery, trafficking, forced labour, child labour, involuntary prison labour or labour rights abuses by it or its sub-contractors to the Authority and the Modern Slavery Helpline and relevant national or local law enforcement agencies;
- (l) if the Supplier is in Default under Clauses 33.8(a) to 33.8(k) the Authority may by notice:
 - (i) require the Supplier to remove from performance of the Contract any sub-contractor, Supplier Personnel or other persons associated with it whose acts or omissions have caused the Default; or
 - (ii) immediately terminate the Contract in accordance with Clause 31.1(b); and
- (m) shall, if the Supplier or the Authority identifies any occurrence of modern slavery connected to this Contract, comply with any request of the Authority to follow the Rectification Plan Process to submit a remedial action plan which follows the form set out in Annex D of the Tackling Modern Slavery in Government Supply Chains guidance to PPN 02/23 (Tackling Modern Slavery in Government Supply Chains);
- (n) shall comply with any request by the Authority to complete the Modern Slavery Assessment Tool within sixty (60) days of such request;
- (o) shall comply with any request by the Authority to provide a Supply Chain Map within fourteen (14) days of such request;
- (p) shall comply with any request by the Authority to provide a copy of any reports of any sub-contractor regarding any or all of workplace conditions, working or employment practices and recruitment practices within fourteen (14) days of such request;

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (q) shall carry out due diligence to ensure workers in its business and its supply chains are not paying illegal or exploitative recruitment fees to secure employment, and where these fees are uncovered shall ensure that workers are remedied; and
- 33.9 The following shall be added to the definition of “Audit” in Paragraph 1.1 of Schedule 19 (*Financial Reports and Audit Rights*) immediately after limb (t):
- “(u) to carry out an unannounced or semi-announced inspection of any Site and speak directly to any Supplier Personnel in a confidential manner and in the native language of such Supplier Personnel in respect of workforce conditions, working or employment practices and recruitment practices;”
- 33.10 For the purposes of an audit carried out pursuant to limb (u) of the definition of “Audit”, in addition to any other rights under the Contract, the Authority may instruct the Supplier to carry out such an audit of any Sub-Contractor by an independent third party and, if so instructed, the Supplier shall deliver a report to the Authority within ninety (90) days of such instruction.
- 33.11 If the Supplier notifies the Authority pursuant to Clause 33.13 it shall respond promptly to the Authority’s enquiries, co-operate with any investigation, and allow the Authority to audit any books, records and/or any other relevant documentation in accordance with the Contract.
- 33.12 If the Supplier is in Default under Clause 33.8 the Authority may by notice:
- (a) require the Supplier to remove from performance of the Contract any Sub-Contractor, Supplier Personnel or other persons associated with it whose acts or omissions have caused the Default; or
 - (b) immediately terminate the Contract in accordance with Clause 31.1(b).

Whistleblowing

- 33.13 As soon as it is aware of it the Supplier and Supplier Personnel must report to the Authority any actual or suspected breach of:
- (a) Law;
 - (b) Clauses 33.1 to 33.8 or 33.14; or
 - (c) Clause 37.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 33.14 The Supplier must not retaliate against any of the Supplier Personnel who in good faith reports a breach listed in this Clause to the Authority or a Prescribed Person.

34 ASSIGNMENT AND NOVATION

- 34.1 The Supplier shall not assign, novate or otherwise dispose of or create any trust in relation to any or all of its rights, obligations or liabilities under this Contract without the prior written consent of the Authority.
- 34.2 The Authority may at its discretion assign, novate or otherwise dispose of any or all of its rights, obligations and liabilities under this Contract and/or any associated licences to:
- (a) any Crown Body; or
 - (b) to a body other than a Crown Body (including any private sector body) which performs any of the functions that previously had been performed by the Authority,

and the Supplier shall, at the Authority's request, enter into a novation agreement in such form as the Authority shall reasonably specify in order to enable the Authority to exercise its rights pursuant to this Clause 34.2.

- 34.3 A change in the legal status of the Authority such that it ceases to be a Crown Body shall not (subject to Clause 34.4) affect the validity of this Contract and this Contract shall be binding on any successor body to the Authority.
- 34.4 If the Authority assigns, novates or otherwise disposes of any of its rights, obligations or liabilities under this Contract to a body which is not a Crown Body or if a body which is not a Crown Body succeeds the Authority (any such body a "**Successor Body**"), the Supplier shall have the right to terminate for an Insolvency Event affecting the Successor Body identical to the right of termination of the Authority under limb (k) of the definition of Supplier Termination Event (as if references in that limb (k) to the Supplier were references to the Successor Body) and the consequences of termination set out in Clause 32.3 shall apply.

35 WAIVER AND CUMULATIVE REMEDIES

- 35.1 The rights and remedies under this Contract may be waived only by notice and in a manner that expressly states that a waiver is intended. A failure or delay by a Party in ascertaining or exercising a right or remedy provided under this Contract or by law shall not constitute a waiver of that right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.
- 35.2 Unless otherwise provided in this Contract, rights and remedies under this Contract are cumulative and do not exclude any rights or remedies provided by law, in equity or otherwise.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

36 RELATIONSHIP OF THE PARTIES

- 36.1 Except as expressly provided otherwise in this Contract, nothing in this Contract, nor any actions taken by the Parties pursuant to this Contract, shall create a partnership, joint venture or relationship of employer and employee or principal and agent between the Parties, or authorise either Party to make representations or enter into any commitments for or on behalf of any other Party.

37 PREVENTION OF FRAUD AND BRIBERY

- 37.1 The Supplier represents and warrants that neither it, nor to the best of its knowledge any Supplier Personnel, have at any time prior to the Effective Date:

- (a) committed a Prohibited Act or been formally notified that it is subject to an investigation or prosecution which relates to an alleged Prohibited Act; and/or
- (b) been listed by any government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in government procurement programmes or contracts on the grounds of a Prohibited Act.

- 37.2 The Supplier shall not during the term of this Contract:

- (a) commit a Prohibited Act; and/or
- (b) do or suffer anything to be done which would cause the Authority or any of the Authority's employees, consultants, contractors, sub-contractors or agents to contravene any of the Relevant Requirements or otherwise incur any liability in relation to the Relevant Requirements.

- 37.3 The Supplier shall during the term of this Contract:

- (a) establish, maintain and enforce, and require that its Sub-contractors establish, maintain and enforce, policies and procedures which are adequate to ensure compliance with the Relevant Requirements and prevent the occurrence of a Prohibited Act;
- (b) have in place reasonable prevention measures (as defined in sections 45(3) and 46(4) of the Criminal Finance Act 2017) to ensure that Associated Persons of the Supplier do not commit tax evasion facilitation offences as defined under that Act;
- (c) keep appropriate records of its compliance with its obligations under Clause 37.3(a) and make such records available to the Authority on request; and
- (d) take account of any guidance about preventing facilitation of tax evasion offences which may be published and updated in accordance with Section 47 of the Criminal Finances Act 2017.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 37.4 The Supplier shall immediately notify the Authority in writing if it becomes aware of any breach of Clause 37.1 and/or 37.2, or has reason to believe that it has or any of the Supplier Personnel have:
- (a) been subject to an investigation or prosecution which relates to an alleged Prohibited Act;
 - (b) been listed by any government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in government procurement programmes or contracts on the grounds of a Prohibited Act; and/or
 - (c) received a request or demand for any undue financial or other advantage of any kind in connection with the performance of this Contract or otherwise suspects that any person or Party directly or indirectly connected with this Contract has committed or attempted to commit a Prohibited Act.
- 37.5 If the Supplier makes a notification to the Authority pursuant to Clause 37.4, the Supplier shall respond promptly to the Authority's enquiries, co-operate with any investigation, and allow the Authority to Audit any books, Records and/or any other relevant documentation in accordance with Clause 12 (*Records, Reports, Audits and Open Book Data*).
- 37.6 If the Supplier is in Default under Clauses 37.1 and/or 37.2, the Authority may by notice:
- (a) require the Supplier to remove from performance of this Contract any Supplier Personnel whose acts or omissions have caused the Default; or
 - (b) immediately terminate this Contract in accordance with Clause 31.1(b).
- 37.7 Any notice served by the Authority under Clause 37.6 shall specify the nature of the Prohibited Act, the identity of the Party who the Authority believes has committed the Prohibited Act and the action that the Authority has elected to take (including, where relevant, the date on which this Contract shall terminate).

38 SEVERANCE

- 38.1 If any provision or part provision of this Contract is or becomes invalid, illegal or unenforceable for any reason, such provision or part provision shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this Contract.

39 FURTHER ASSURANCES

- 39.1 Each Party undertakes at the request of the other, and at the cost of the requesting Party to do all acts and execute all documents which may be reasonably necessary to give effect to the meaning of this Contract.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

40 ENTIRE AGREEMENT

- 40.1 This Contract constitutes the entire agreement between the Parties in respect of its subject matter and supersedes and extinguishes all prior negotiations, arrangements, understanding, course of dealings or agreements made between the Parties in relation to its subject matter, whether written or oral.
- 40.2 Neither Party has been given, nor entered into this Contract in reliance on, any warranty, statement, promise or representation other than those expressly set out in this Contract.
- 40.3 Nothing in this Clause 40 shall exclude any liability in respect of misrepresentations made fraudulently.

41 THIRD PARTY RIGHTS

- 41.1 The provisions of Clause 17.1 (*IPRs Indemnity*), Paragraphs 2.1, 2.6, 3.1 and 3.3 of Part B, Paragraphs 2.1 and 2.3 of Part C, Part D and Paragraphs 1.4, 2.3 and 2.8 of Part E of Schedule 28 (*Staff Transfer*) and the provisions of Paragraph 7.9 of Schedule 25 (*Exit Management*) (together “**Third Party Provisions**”) confer benefits on persons named or identified in such provisions other than the Parties (each such person a “**Third Party Beneficiary**”) and are intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.
- 41.2 Subject to Clause 41.1, a person who is not a Party to this Contract has no right under the CRTPA to enforce any term of this Contract but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.
- 41.3 No Third Party Beneficiary may enforce, or take any step to enforce, any Third Party Provision without the prior written consent of the Authority, which may, if given, be given on and subject to such terms as the Authority may determine.
- 41.4 Any amendments or modifications to this Contract may be made, and any rights created under Clause 41.1 may be altered or extinguished, by the Parties without the consent of any Third Party Beneficiary.

42 NOTICES

- 42.1 Any notices sent under this Contract must be in writing.
- 42.2 Subject to Clause 42.4, the following table sets out the method by which notices may be served under this Contract and the respective deemed time and proof of service:

Manner of Delivery	Deemed service	time	of	Proof of service

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Email	9.00am on the first Working Day after sending	Dispatched as a pdf attachment to an e-mail to the correct e-mail address without any error message.
Personal delivery	On delivery, provided delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the next Working Day.	Properly addressed and delivered as evidenced by signature of a delivery receipt
Prepaid, Royal Mail Signed For™ 1st Class or other prepaid, next Working Day service providing proof of delivery.	At the time recorded by the delivery service, provided that delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the same Working Day (if delivery before 9.00am) or on the next Working Day (if after 5.00pm).	Properly addressed prepaid and delivered as evidenced by signature of a delivery receipt

- 42.3 Notices shall be sent to the addresses set out below or at such other address as the relevant Party may give notice to the other Party for the purpose of service of notices under this Contract:

	Supplier	Authority
Contact	VodafoneThree - UK Legal Team	Contract Manager
Address	The Connection Vodafone House Newbury Berkshire RG14 2FN	Zone 3.19, 3rd Floor, 10 South Colonnade, Canary Wharf E14 4PU
Email	[REDACTED] and [REDACTED]	vvn.cmo@justice.gov.uk

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 42.4 The following notices may only be served as an attachment to an email if the original notice is then sent to the recipient by personal delivery or recorded delivery in the manner set out in the table in Clause 42.2:
- (a) Step-In Notices;
 - (b) Force Majeure Notices;
 - (c) notices issued by the Supplier pursuant to Clause 31.3 (*Termination by the Supplier*);
 - (d) Termination Notices; and
 - (e) Dispute Notices.
- 42.5 Failure to send any original notice by personal delivery or recorded delivery in accordance with Clause 42.4 shall invalidate the service of the related e-mail transmission. The deemed time of delivery of such notice shall be the deemed time of delivery of the original notice sent by personal delivery or Royal Mail Signed For™ 1st Class delivery (as set out in the table in Clause 42.2) or, if earlier, the time of response or acknowledgement by the other Party to the email attaching the notice.
- 42.6 This Clause 42 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution (other than the service of a Dispute Notice under Schedule 23 (*Dispute Resolution Procedure*)).

43 DISPUTES

- 43.1 The Parties shall resolve Disputes arising out of or in connection with this Contract in accordance with the Dispute Resolution Procedure.
- 43.2 The Supplier shall continue to provide the Services in accordance with the terms of this Contract until a Dispute has been resolved.

44 GOVERNING LAW AND JURISDICTION

- 44.1 This Contract and any issues, disputes or claims (whether contractual or non-contractual) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws of England and Wales.
- 44.2 Subject to Clause 43 (*Disputes*) and Schedule 23 (*Dispute Resolution Procedure*) (including the Authority's right to refer the dispute to arbitration), the Parties agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (whether contractual or non-contractual) that arises out of or in connection with this Contract or its subject matter or formation.

CORE TERMS

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

This Contract has been duly entered into by the Parties on the date which appears at the head of its page 1.

SIGNED for and on behalf of)
VODAFONE LIMITED by a director:)
)
)

Signature:

[REDACTED]

Name

(block capitals): [REDACTED]

Director

SIGNED for and on behalf of)
THE SECRETARY OF STATE)
FOR JUSTICE)
)

Signature:

[REDACTED]

Name

(block capitals): [REDACTED]

Position: [REDACTED]

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SCHEDULE 1

DEFINITIONS

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Schedule 1 (*Definitions*)**1 DEFINITIONS**

- 1.1 In the Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Schedule 1 (*Definitions*) or the relevant Schedule in which that capitalised expression appears.
- 1.2 If a capitalised expression does not have an interpretation in this Schedule or any other Schedule, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.
- 1.3 In the Contract, unless the context otherwise requires:
- 1.3.1 the singular includes the plural and vice versa;
 - 1.3.2 reference to a gender includes the other gender and the neuter;
 - 1.3.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Crown Body;
 - 1.3.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;
 - 1.3.5 the words "**including**", "**other**", "**in particular**", "**for example**" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "**without limitation**";
 - 1.3.6 references to "**writing**" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;
 - 1.3.7 references to "**representations**" shall be construed as references to present facts, to "**warranties**" as references to present and future facts and to "**undertakings**" as references to obligations under the Contract;
 - 1.3.8 references to "**Clauses**" and "**Schedules**" are, unless otherwise provided, references to the clauses and schedules of the Core Terms and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;

SCHEDULE 1 (DEFINITIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 1.3.9 references to **"Paragraphs"** are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided;
- 1.3.10 references to a series of Clauses or Paragraphs shall be inclusive of the clause numbers specified;
- 1.3.11 the headings in the Contract are for ease of reference only and shall not affect the interpretation or construction of the Contract;
- 1.3.12 where the Buyer is a Crown Body, it shall be treated as contracting with the Crown as a whole; and
- 1.3.13 the expressions listed in ITIL shall have the meanings given to them in ITIL and this shall also apply to ITIL expressions that may be used in this Contract with a capital first letter, but which are listed in ITIL with a lower-case first letter.
- 1.4 Any reference in this Contract which immediately before IP Completion Day (or such later date when relevant EU law ceases to have effect pursuant to Section 1A of the European Union (Withdrawal) Act 2018) is a reference to (as it has effect from time to time):
- 1.4.1 any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement (**"EU References"**) which is to form part of domestic law by application of Section 3 of the European Union (Withdrawal) Act 2018 shall be read on and after IP Completion Day as a reference to the EU References as they form part of domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 as modified by domestic law from time to time; and
- 1.4.2 any EU institution or EU authority or other such EU body shall be read on and after IP Completion Day as a reference to the UK institution, authority or body to which its functions were transferred.
- 1.5 Where a standard, policy or document is referred to in this Contract by reference to a hyperlink, then if the hyperlink is changed or no longer provides access to the relevant standard, policy or document, the Supplier shall notify the Authority and the Parties shall update this Contract with a reference to the replacement hyperlink.
- 1.6 If there is any conflict between the meaning given to an expression in ITIL and the meaning given to the expression in this Schedule 1 (*Definitions*), then the meaning given to that expression in this Schedule 1 (*Definitions*) shall apply. Paragraph 1.3.13 shall apply to ITIL expressions that may be used in this Contract with a capital first letter, but which are listed in ITIL with a lower-case first letter.
- "4G"** means the fourth-generation technology standard for mobile networks;
- "5G"** means the fifth-generation technology standard for mobile networks;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Access Circuit”	means a physical link installed at an Authority Site which provides access to a network such as the internet;
“Accounting Reference Date”	means in each year the date to which the Supplier prepares its annual audited financial statements;
“Achieve”	(a) in respect of a Test, to successfully pass a Test without any Test Issues; and (b) in respect of a Milestone, the issue of a Milestone Achievement Certificate in respect of that Milestone in accordance with the provisions of Schedule 14 (<i>Testing Procedures</i>), and “Achieved” , and “Achievement” shall be construed accordingly;
“Affected Party”	the Party seeking to claim relief in respect of a Force Majeure Event;
“Affiliate”	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time;
“Agreed Transfer Date”	has the meaning given in Part B of Schedule 11 (<i>Third Party Contracts</i>);
“Allowable Assumptions”	the assumptions set out in Annex 5 of Schedule 15 (<i>Charges and Invoicing</i>);
“Allowable Price”	in relation to the Retained Deliverables relating to a CPP Milestone, if any, an amount determined in accordance with the formula: A – B where: (a) A is an amount equal to the Costs incurred by the Supplier in providing or developing the relevant Retained Deliverables as reflected in the

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Financial Model together with an amount equal to the Anticipated Contract Life Profit Margin thereon; and

- (b) B is an amount equal to the Allowable Price Adjustment relating to the relevant Retained Deliverables, if any, or if there is no such Allowable Price Adjustment, zero,

provided that the Allowable Price for any Retained Deliverables shall in no circumstances exceed the aggregate amount of the Milestone Payments paid to the Supplier in respect of the Milestones (or in the case of Partial Termination, the Milestones for the parts of the Services terminated) relating to that CPP Milestone;

“Allowable Price Adjustment”

has the meaning given in Clause 32.8(c) (Payments by the Supplier);

“Ancillary Fixed Broadband Services”

as described in requirement 3.2.4.3 of the Technical Requirements;

“Annual Contract Report”

has the meaning given in Schedule 19 (*Financial Reports and Audit Rights*);

“Annual Revenue”

means, for the purposes of determining whether an entity is a Public Sector Dependent Supplier, the audited consolidated aggregate revenue (including share of revenue of joint ventures and Associates) reported by the Supplier or, as appropriate, the Supplier Group in its most recent published accounts, subject to the following methodology:

- (a) figures for accounting periods of other than 12 months should be scaled pro rata to produce a proforma figure for a 12 month period; and
- (b) where the Supplier, the Supplier Group and/or their joint ventures and Associates report in a foreign currency, revenue should be converted to British Pound Sterling at

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

the closing exchange rate on the
Accounting Reference Date;

“Anticipated Contract Life Profit Margin”	has the meaning given in Schedule 15 (<i>Charges and Invoicing</i>);
“Approval”	means, in respect of a Documentary Deliverable, to successfully meet its Quality Criteria and have an Approval Certificate issued, and “Approve” and “Approved” shall be construed accordingly;
“Approval Certificate”	a certificate supplied by the Authority when a Documentary Deliverable meets all its Quality Criteria;
"Approval Failure"	has the meaning given in Paragraph 1.27.1 of Part B of Schedule 13 (<i>Implementation Plan</i>);
"Approval Success"	has the meaning given in Paragraph 1.26.1 of this Part B of Schedule 13 (<i>Implementation Plan</i>);
“Approved Sub-Licensee”	any of the following: (a) a Crown Body; (b) any third party providing services to a Crown Body; and/or (c) any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Authority;
“Artefact Description”	(a) a document describing a project Deliverable in the form set out in Annex 2 of Schedule 13 (<i>Implementation Plan</i>) and according to content specified by the Authority; or (b) a description of a product's purpose, composition, derivation and quality criteria, produced at planning time, once the need for the product is

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

identified, in a form and according to
content specified by the Authority;

“Assets”	all assets and rights used by the Supplier to provide the Services in accordance with this Contract but excluding the Authority Assets;
“Associated Person”	has the meaning given to it in Section 44(4) of the Criminal Finances Act 2017;
“Associates”	means, in relation to an entity, an undertaking in which the entity owns, directly or indirectly, between 20% and 50% of the voting rights and exercises a degree of control sufficient for the undertaking to be treated as an associate under generally accepted accounting principles;
“Assurance”	means written confirmation from a Relevant Authority to the Supplier that the CRP Information is approved by the Relevant Authority;
“ATP Milestone”	the Milestone linked to Authority to Proceed for the relevant Operational Services set out in the Implementation Plan;
“Audit”	any exercise by the Authority of its Audit Rights pursuant to Clause 12 (Records, Reports, Audit and Open Book Data) and Schedule 19 (<i>Financial Reports and Audit Rights</i>);
“Audit Agents”	(a) the Authority’s internal and external auditors; (b) the Authority’s statutory or regulatory auditors; (c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; (d) HM Treasury or the Cabinet Office;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (e) any party formally appointed by the Authority to carry out audit or similar review functions; and
- (f) successors or assigns of any of the above;

“Audit Rights”

the audit and access rights referred to in Schedule 19 (*Financial Reports and Audit Rights*);

“Authority Assets”

the Authority Materials, the Authority infrastructure and any other data, software, assets, equipment or other property owned by and/or licensed or leased to the Authority and which is or may be used in connection with the provision or receipt of the Services;

“Authority Background IPRs”

- (a) IPRs owned by the Authority and/or a Service Recipient before the Effective Date, including IPRs contained in any of the Authority's Know-How, documentation, processes and procedures;
- (b) IPRs created by the Authority and/or a Service Recipient independently of this Contract; and/or
- (c) Crown Copyright which is not available to the Supplier otherwise than under this Contract;

but excluding IPRs owned by the Authority and/or a Service Recipient subsisting in the Authority Software;

“Authority Cause”

any material breach by the Authority of any of the Authority Responsibilities, except to the extent that such breach is:

- (a) the result of any act or omission by the Authority to which the Supplier has given its prior consent; or
- (b) caused by the Supplier, any Sub-contractor or any Supplier Personnel;

“Authority Comms Room”

means a room at an Authority Site that houses devices and equipment necessary to

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

deliver End to End Services at the Authority Sites;

“Authority Data”

- (a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are:
 - (i) supplied to the Supplier by or on behalf of the Authority and/or a Service Recipient; and/or
 - (ii) which the Supplier is required to generate, process, store or transmit pursuant to this Contract; or
- (b) any Personal Data for which the Authority and/or a Service Recipient is the Controller;

“Authority Data Centres”

means the data centres used by the Authority in the delivery of its ICT services;

“Authority IT Strategy”

the Authority's digital strategy at the Effective Date, which can be found at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1064860/moj-digital-strategy-2025.pdf;

“Authority Materials”

the Authority Data together with any materials, documentation, information, programs and codes supplied by the Authority and/or a Service Recipient to the Supplier, the IPRs in which:

- (a) are owned or used by or on behalf of the Authority and/or a Service Recipient; and
- (b) are or may be used in connection with the provision or receipt of the Services,

but excluding any Project Specific IPRs, Specially Written Software, Supplier

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	Software, Third Party Software and Documentation relating to Supplier Software or Third Party Software;
“Authority Premises”	premises owned, controlled or occupied by the Authority, a Service Recipient and/or any Crown Body which are made available for use by the Supplier or its Sub-contractors for provision of the Services (or any of them);
“Authority Representative”	the representative appointed by the Authority pursuant to Clause 11.4 (Representatives);
“Authority Requirements”	the requirements of the Authority set out in Schedule 2 (<i>Services Description</i>)), Schedule 3 (<i>Performance Levels</i>), Schedule 4 (<i>Standards</i>), Schedule 5 (<i>Security Management</i>), Schedule 6 (<i>Insurance Requirements</i>), Schedule 13 (<i>Implementation Plan</i>), Schedule 24 (<i>Reports and Records Provisions</i>), Schedule 25 (<i>Exit Management</i>), Schedule 26 (<i>Service Continuity Plan and Corporate Resolution Planning</i>) and Schedule 34 (<i>Transitional Services</i>);
“Authority Responsibilities”	the responsibilities of the Authority specified in Schedule 7 (<i>Authority Responsibilities</i>);
“Authority Secure Disposal of IT Equipment Policy”	the Authority’s secure disposal of IT equipment policy as stated at https://security-guidance.service.justice.gov.uk/secure-disposal-of-it-equipment/#secure-disposal-of-it-equipment ;
“Authority’s Service Desk”	the service desk as provided by the Authority (for example, via an Other Supplier) to deal with End User queries including Incidents and Requests;
“Authority Site”	the Authority’s and/or Service Recipients’ sites at which the Operational Services are delivered, including those listed on the Authority Site List;
“Authority Site Access Request Process”	has the meaning given in requirement 7.2.1.18 of the Transition Requirements;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Authority Site List”	means the information set out in the ITSM Toolset listing the Authority Sites;
“Authority Site Specification”	means the information set out in the ITSM Toolset listing the Authority Sites and the Authority’s WAN specification;
“Authority Software”	software which is owned by or licensed to the Authority and/or a Service Recipient (other than under or pursuant to this Contract) and which is or will be used by the Supplier for the purposes of providing the Services;
“Authority System”	the Authority’s computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Authority and/or a Service Recipient or the Supplier in connection with this Contract which is owned by the Authority and/or a Service Recipient or licensed to it and/or a Service Recipient by a third party and which interfaces with the Supplier System or which is necessary for the Authority and/or a Service Recipient to receive the Services;
“Authority to Proceed” or “ATP”	means the authorisation to the Supplier to commence the provision of the relevant Operational Services to the Authority, provided by the Authority in the form of a Milestone Achievement Certificate in respect of the ATP Milestone;
“Availability”	has the meaning given in Schedule 3 (<i>Performance Levels</i>);
“Availability Management System”	means those processes, tools and data used in the ITSM Toolset for the purpose of managing Availability;
“Balanced Scorecard Report”	has the meaning given in Paragraph 1.3 of Part B of Schedule 3 (<i>Performance Levels</i>);
“Baseline Security Requirements”	has the meaning given in Schedule 5 (<i>Security Management</i>);
“Board”	means the Supplier’s board of directors;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Board Confirmation”	means the written confirmation from the Board in accordance with Paragraph 8 of Schedule 18 (<i>Financial Distress</i>);
“Breakage Costs Payment”	has the meaning given in Schedule 16 (<i>Payments on Termination</i>);
“Bronze Site”	means an Authority Site which is specified as being a Bronze Site in the Authority Site List and in the reasonable opinion of the Authority has a lower level of business criticality;
“Cabinet Office Markets and Suppliers Team”	means the UK Government’s team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function;
“Capacity Management Policies”	means the Authority’s capacity management policies as notified by the Authority to the Supplier from time to time;
“Capacity Management Services”	has the meaning given in requirement 6.3.2.1 of the Service Management Requirements;
“Capacity Plan”	has the meaning given in requirement 6.3.2.6 of the Service Management Requirements;
“Capacity Report”	has the meaning given in requirement 6.3.2.5 of the Service Management Requirements;
“Catalogue Item”	means a product or service described within the Product and Service Catalogue;
“CDR”	means committed data rate;
“Certificate of Costs”	has the meaning given in Schedule 15 (<i>Charges and Invoicing</i>);
“Change”	any change to this Contract;
“Change Advisory Board” or “CAB”	has the meaning given in requirement 6.4.1.10 of the Service Management Requirements and as further elaborated in the Processes;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Change and Evaluation Management”	means the Process of the same name listed in Paragraph 12.1 of Schedule 4 (<i>Standards</i>);
“Change Authorisation Note”	a form setting out an agreed Contract Change which shall be substantially in the form of Annex 2 (Change Authorisation Note) to Part A of Schedule 22 (<i>Change Control Procedure, Service Requests and Projects</i>);
“Change Control Procedure”	the procedure for changing this Contract set out in Part A of Schedule 22 (<i>Change Control Procedure, Service Requests and Projects</i>);
“Change in Law”	any change in Law which impacts on the performance of the Services which comes into force after the Effective Date;
“Change Management System”	means those processes, tools and data used in the ITSM Toolset for the purpose of managing Service Changes;
“Change Request”	a written request for a Contract Change substantially in the form of Annex 1 (Change Request Form);
“Charges”	the charges for the provision of the Services set out in or otherwise calculated in accordance with Schedule 15 (<i>Charges and Invoicing</i>) including any Milestone Payment or Service Charge;
“CHECK Service Provider”	has the meaning given in Paragraph 1 of Part A of Schedule 5 (<i>Security Management</i>);
“Civil Works”	means the installation of infrastructure which will house the network cables and equipment. Examples of this would be duct structures, cable chambers, vaults, tap boxes, foundations, handwells and poles;
“Class 1 Transaction”	has the meaning set out in the listing rules issued by the UK Listing Authority;
“CNI”	means Critical National Infrastructure;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Commercially Sensitive Information”	the information listed in Schedule 9 (<i>Commercially Sensitive Information</i>) comprising the information of a commercially sensitive nature relating to: (a) the pricing of the Services; (b) details of the Supplier’s IPRs; and (c) the Supplier’s business and investment plans; which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss;
“Comparable Supply”	the supply of services to another customer of the Supplier that are the same or similar to any of the Services;
“Compensation for Unacceptable KPI Failure”	has the meaning given in Clause 7.4(a) (<i>Unacceptable KPI Failure</i>);
“Compensation Payment”	has the meaning given in Schedule 16 (<i>Payments on Termination</i>);
“Condition Precedent”	has the meaning given in Clause 4.2 (<i>Condition Precedent</i>);
“Confidential Information”	(a) Information, including all Personal Data, which (however it is conveyed) is provided by the Disclosing Party pursuant to or in anticipation of this Contract that relates to: (i) the Disclosing Party Group; or (ii) the operations, business, affairs, developments, intellectual property rights, trade secrets, know-how and/or personnel of the Disclosing Party Group; (b) other Information provided by the Disclosing Party pursuant to or in anticipation of this Contract that is clearly designated as being

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

confidential or equivalent or that ought reasonably to be considered to be confidential (whether or not it is so marked) which comes (or has come) to the Recipient's attention or into the Recipient's possession in connection with this Contract;

- (c) discussions, negotiations, and correspondence between the Disclosing Party or any of its directors, officers, employees, consultants or professional advisers and the Recipient or any of its directors, officers, employees, consultants and professional advisers in connection with this Contract and all matters arising therefrom; and
- (d) Information derived from any of the above,

but not including any Information which:

- (i) was in the possession of the Recipient without obligation of confidentiality prior to its disclosure by the Disclosing Party;
- (ii) the Recipient obtained on a non-confidential basis from a third party who is not, to the Recipient's knowledge or belief, bound by a confidentiality agreement with the Disclosing Party or otherwise prohibited from disclosing the information to the Recipient;
- (iii) was already generally available and in the public domain at the time of disclosure otherwise than by a breach of this Contract or breach of a duty of confidentiality;
- (iv) was independently developed without access to the Confidential Information; or

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (v) relates to the Supplier's:
 - (1) performance under this Contract; or
 - (2) failure to pay any Sub-contractor as required pursuant to Clause 15.15(a) (Supply Chain Protection);

“Configuration Item”	means any Services component, infrastructure element, or other item that needs to be managed in order to ensure the successful delivery of the Services;
“Conflict of Interest”	a conflict between the financial or personal duties of the Supplier or the Supplier Personnel and the duties owed to the Authority under the Contract, in the reasonable opinion of the Authority;
“Contract”	the contract between the Authority and the Supplier;
“Connectivity Services”	means the management of carrier suppliers as detailed in Paragraph 6.8.3 of the Service Management Requirements;
“Continual Service Improvement” or “CSI”	means the process that ensures the performance of the Services is regularly improved, as detailed in requirements 6.5.5.7 to 6.5.6.4 of the Service Management Requirements;
“Continual Service Improvement System”	means the processes, tools and data used in the ITSM Toolset or other Authority system for the purpose of managing Continual Service Improvement;
“Contract Change”	any change to this Contract other than an Operational Change;
“Contract Inception Report”	the initial financial model in a form agreed by the Supplier and the Authority in writing on or before the Effective Date;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Contracts Finder”	the online government portal which allows suppliers to search for information about contracts as prescribed by Part 4 of the Public Contract Regulations 2015;
“Contract Year”	(a) a period of 12 months commencing on the Effective Date; or (b) thereafter a period of 12 months commencing on each anniversary of the Effective Date; provided that the final Contract Year shall end on the expiry or termination of the Term;
“Control”	the possession by person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “Controls” and “Controlled” shall be interpreted accordingly;
“Controller”	has the meaning given in the UK GDPR or the EU GDPR as the context requires;
“Core Information Management System” or “CIMS”	has the meaning given in Paragraph 1 of Part A of Schedule 5 (<i>Security Management</i>);
“Core Network Services”	means the Services described in Paragraph 5 of the Technical Requirements;
“Corporate Change Event”	means: (a) any change of Control of the Supplier or a Parent Undertaking of the Supplier; (b) any change of Control of any member of the Supplier Group which, in the reasonable opinion of the Authority, could have a material adverse effect on the Services; (c) any change to the business of the Supplier or any member of the Supplier Group which, in the reasonable opinion of the Authority,

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

could have a material adverse effect on the Services;

- (d) a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the London Stock Exchange plc;
- (e) an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking place in respect of the Supplier or any Parent Undertaking of the Supplier;
- (f) payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the Net Asset Value of the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any 12 month period;
- (g) an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group;
- (h) any member of the Supplier Group stopping payment of its debts generally or becoming unable to pay its debts within the meaning of section 123(1) of the Insolvency Act 1986 or any member of the Supplier Group ceasing to carry on all or substantially all its business, or any compromise, composition, arrangement or agreement being made with creditors of any member of the Supplier Group;
- (i) the appointment of a receiver, administrative receiver or administrator in respect of or over all or a material part of the undertaking or assets of any member of the Supplier Group; and/or
- (j) any process or events with an effect analogous to those in Paragraphs (e) to (g) inclusive above occurring to a member of the Supplier Group in a

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

jurisdiction outside England and
Wales;

**“Corporate Change Event
Grace Period”**

means a grace period agreed to by the Relevant Authority for providing CRP Information and/or updates to Service Continuity Plan after a Corporate Change Event;

**“Corporate Resolvability
Assessment (Structural
Review)”**

means part of the CRP Information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 2 and Annex 2: Corporate Resolvability Assessment (Structural Review) of Schedule 26 (*Service Continuity Plan and Corporate Resolution Planning*);

“Costs”

has the meaning given in Schedule 15 (*Charges and Invoicing*);

“CPE”

stands for “customer premise equipment” and means Supplier Equipment which is part of the Supplier System and is installed at Authority Sites;

“CPP Milestone”

a contract performance point as set out in the Implementation Plan, being the Milestone at which the Supplier has demonstrated that the Supplier Solution or relevant Service is working satisfactorily in its operating environment in accordance with Schedule 14 (*Testing Procedures*);

**“Critical National
Infrastructure”**

means those critical elements of UK national infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

- (a) major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	(b) significant impact on the national security, national defence, or the functioning of the UK;
“Critical Performance Failure”	(a) the Supplier accruing in aggregate 3140 or more Service Points (in terms of the number of points allocated) in any period of 2 months; or (b) the Supplier accruing Service Credits which meet or exceed the Service Credit Cap in more than six of the Service Periods in any consecutive 12 month period; or (c) the Supplier failing to meet the same KPI Service Threshold on three (3) occasions in six (6) consecutive Service Periods; or (d) the Supplier accruing Compensation for Unacceptable KPI Failure which meets or exceeds the limit set out in Clause 23.4(c)(ii);
“Critical Service Contract”	means the overall status of the Services provided under this Contract as determined by the Authority and specified in Paragraph 1.1 of Part B to Schedule 26 (<i>Service Continuity Plan and Corporate Resolution Planning</i>);
“Crown Body”	means the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the Welsh Government), including government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
“Crown Copyright”	has the meaning given in the Copyright, Designs and Patents Act 1988;
“CRP Information”	means the Corporate Resolution Planning Information, together, the: (a) Exposure Information (Contracts List);

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	(b) Corporate Resolvability Assessment (Structural Review); and
	(c) Financial Information and Commentary;
“CRTPA”	the Contracts (Rights of Third Parties) Act 1999;
“Cyber and Technical Security Guidance”	means the Authority’s cyber and technical security guidance found at https://security-guidance.service.justice.gov.uk/#cyber-and-technical-security-guidance and as updated from time to time;
“Data Loss Event”	any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;
“Data Protection Impact Assessment”	an assessment by the Controller carried out in accordance with section 3 of Chapter IV of the UK GDPR and sections 64 and 65 of the DPA 2018;
“Data Protection Legislation”	(a) all applicable UK law relating to the processing of personal data and privacy, including but not limited to the UK GDPR, and the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy; and (b) (to the extent that it may be applicable) the EU GDPR). The UK GDPR and EU GDPR are defined in section 3 of the Data Protection Act 2018;
“Data Room”	means the repository of documents included in the eSourcing Portal during the procurement process containing data and information to assist the Bidders in understanding the Services and support the preparation of their responses to the SQ, ISOS, draft ISDS, ISDS and ISFT;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Data Subject”	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
“Data Subject Request”	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to their Personal Data;
“DC Interconnect”	has the meaning given in requirement 4.3.1.1 of the Technical Requirements;
“DC Load Balancers”	has the meaning given in requirement 4.3.1.1 of the Technical Requirements;
“DC Transit LAN”	has the meaning given in requirement 4.3.1.1 of the Technical Requirements;
“Deductions”	all Service Credits, Compensation for Unacceptable KPI Failure, Delay Payments or any other deduction which is paid or payable to the Authority under this Contract;
“Default”	any breach of the obligations of the relevant Party (including abandonment of this Contract in breach of its terms, repudiatory breach or breach of a fundamental term) or any other default, act, omission, negligence or statement: (a) in the case of the Authority, of its employees, servants, agents; or (b) in the case of the Supplier, of its Sub-contractors or any Supplier Personnel, in connection with or in relation to the subject-matter of this Contract and in respect of which such Party is liable to the other;
“Defect”	(a) any error, damage or defect in the manufacturing of a Deliverable; or (b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or (c) any failure of any Deliverable to provide the performance, features and

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	functionality specified in the Authority Requirements or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from meeting its associated Test Success Criteria; or
	(d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the Authority Requirements or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from meeting its associated Test Success Criteria;
“Delay”	(a) a delay in the Achievement of a Milestone by its Milestone Date; or (b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan;
“Delay Deduction Period”	the period commencing on the relevant Milestone Date and finishing on the earlier of: (a) the Supplier accruing Delay Payments which in aggregate meet or exceed the Delay Payment Cap; and (b) the expiry of the number of days specified against the relevant Key Milestone in the final column of the table in Annex A to Schedule 15 (<i>Charges and Invoicing</i>);
“Delay Payments”	the amounts payable by the Supplier to the Authority in respect of a Delay in Achieving a Key Milestone as specified in Schedule 15 (<i>Charges and Invoicing</i>);
“Delay Payment Cap”	has the meaning given in Schedule 15 (<i>Charges and Invoicing</i>);

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Deliverable”	an item, feature or software delivered or to be delivered by the Supplier at or before a Milestone Date or at any other stage during the performance of this Contract which may be either a Documentary Deliverable or a Non-Documentary Deliverable;
“Demand Management”	means the methodology as set out in the Demand Management Process to enable the Supplier to plan and manage demand for the Services, on behalf of the Authority;
“Demand Management System”	means the processes, tools and data used in the ITSM Toolset for Demand Management;
“Demand Request”	means a Request for new Services or change to existing Services that is recorded as part of Demand Management;
“Dependent Parent Undertaking”	means any Parent Undertaking which provides any of its Subsidiary Undertakings and/or Associates, whether directly or indirectly, with any financial, trading, managerial or other assistance of whatever nature, without which the Supplier would be unable to continue the day to day conduct and operation of its business in the same manner as carried on at the time of entering into this Contract, including for the avoidance of doubt the provision of the Services in accordance with the terms of this Contract;
“Deployed Architecture”	has the meaning given in requirement 6.7.1.6 of the Service Management Requirements;
“Detailed Implementation Plan”	the plan developed and revised from time to time in accordance with Paragraphs 3 and 4 of Schedule 13 (<i>Implementation Plan</i>);
“Device”	means any device used to deliver the Services, and devices in scope of the SASE Services;
“Device Management”	has the meaning given in requirement 5.5.1.1 of the Technical Requirements;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“DHCP”	means dynamic host control protocol;
“DIA”	means dedicated internet access;
“Disclosing Party”	has the meaning given in Clause 19.1 (<i>Confidentiality</i>);
“Disclosing Party Group”	(a) where the Disclosing Party is the Supplier, the Supplier and any Affiliates of the Supplier; and (b) where the Disclosing Party is the Authority, the Authority and any Crown Body with which the Authority or the Supplier interacts in connection with this Contract;
“Dispute”	any dispute, difference or question of interpretation arising out of or in connection with this Contract, including any dispute, difference or question of interpretation relating to the Services, failure to agree in accordance with the Change Control Procedure or any matter where this Contract directs the Parties to resolve an issue by reference to the Dispute Resolution Procedure;
“Dispute Notice”	a written notice served by one Party on the other stating that the Party serving the notice believes that there is a Dispute;
“Dispute Resolution Procedure”	the dispute resolution procedure set out in Schedule 23 (<i>Dispute Resolution Procedure</i>);
“DLP”	means data loss prevention;
“DNS”	means domain name system;
“Document Approval Procedure”	the procedures for review and Approval of Documentary Deliverables as set out in Paragraph 1 of Part B of Schedule 13 (<i>Implementation Plan</i>);
“Document Review Plan”	a plan for undertaking the review and Approval of a Documentary Deliverable, as

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

described in Paragraph 1 of Part B of
Schedule 13 (*Implementation Plan*);

“Documentary Deliverable” means a Deliverable that takes the form of
Documentation;

“Documentation” descriptions of the Services and
Performance Indicators, details of the
Supplier System (including (i) vendors and
versions for off-the-shelf components and (ii)
source code and build information for
proprietary components), relevant design
and development information, technical
specifications of all functionality including
those not included in standard manuals
(such as those that modify system
performance and access levels),
configuration details, test scripts, user
manuals, operating manuals, process
definitions and procedures, and all such
other documentation as:

- (a) is required to be supplied by the
Supplier to the Authority under this
Contract;
- (b) would reasonably be required by a
competent third party capable of Good
Industry Practice contracted by the
Authority to develop, configure, build,
deploy, run, maintain, upgrade and
test the individual systems that
provide Services;
- (c) is required by the Supplier in order to
provide the Services; and/or
- (d) has been or shall be generated for the
purpose of providing the Services;

“DOM1” means the primary active directory domain
used by the Authority;

“DOTAS” the Disclosure of Tax Avoidance Schemes
rules which require a promoter of tax
schemes to tell HMRC of any specified
notifiable arrangements or proposals and to
provide prescribed information on those
arrangements or proposals within set time

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to national insurance contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868) made under section 132A of the Social Security Administration Act 1992;

“DPA 2018”	the Data Protection Act 2018;
“Due Diligence Information”	any information supplied to the Supplier by or on behalf of the Authority prior to the Effective Date;
“EEA”	European Economic Area;
“Effective Date”	the date on which this Contract is signed by both Parties;
“EIRs”	the Environmental Information Regulations 2004, together with any guidance and/or codes of practice issued by the Information Commissioner or any Crown Body in relation to such Regulations;
“Emergency Maintenance”	ad hoc and unplanned maintenance provided by the Supplier where: (a) the Authority reasonably suspects that the IT Environment or the Services, or any part of the IT Environment or the Services, has or may have developed a fault, and notifies the Supplier of the same; or (b) the Supplier reasonably suspects that the IT Environment or the Services, or any part the IT Environment or the Services, has or may have developed a fault;
“Employee Liabilities”	all claims, actions, proceedings, orders, demands, complaints, investigations (save for any claims for personal injury which are covered by insurance) and any award, compensation, damages, tribunal awards,

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

fine, loss, order, penalty, disbursement, payment made by way of settlement and costs, expenses and legal costs reasonably incurred in connection with a claim or investigation related to employment including in relation to the following:

- (a) redundancy payments including contractual or enhanced redundancy costs, termination costs and notice payments;
- (b) unfair, wrongful or constructive dismissal compensation;
- (c) compensation for discrimination on grounds of sex, race, disability, age, religion or belief, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation or claims for equal pay;
- (d) compensation for less favourable treatment of part-time workers or fixed term employees;
- (e) outstanding employment debts and unlawful deduction of wages including any PAYE and national insurance contributions;
- (f) employment claims whether in tort, contract or statute or otherwise;
- (g) any investigation relating to employment matters by the Equality and Human Rights Commission or other enforcement, regulatory or supervisory body and of implementing any requirements which may arise from such investigation;

“Employment Regulations”

the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced;

[REDACTED]

[REDACTED]

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“End to End Services”	the Services together with all other ICT services supplied to the Authority by the Supplier and Other Suppliers;
“End User”	any person authorised by the Authority and/or Service Recipients to use the IT Environment and/or the Services;
“End User Computing Services (EUCS)”	means the end user computing services provided to the Authority by the EUCS Supplier(s);
“EUCS Supplier”	means the supplier(s) responsible for delivering the End User Computing Services;
“Estimated Year 1 Charges”	the estimated Charges payable by the Authority during the first Contract Year, as set out in the Financial Model;
“Estimated Initial Service Charges”	the estimated Service Charges payable by the Authority during the period of 12 months from the first Operational Service Commencement Date, as set out in the Financial Model;
“EU GDPR”	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it has effect in EU law;
“EU”	European Union;
“Event”	Shall have the meaning given to it in ITIL in accordance with Paragraph 1.3.13 of this Schedule;
“Event Management System”	means the processes, tools and data used for the purpose of managing Events;
“Excess Construction Charges” or “ECCs”	has the meaning given in Schedule 15 (<i>Charges and Invoicing</i>);

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Exit Management”	services, activities, processes and procedures to ensure a smooth and orderly transition of all or part of the Services from the Supplier to the Authority and/or a Replacement Supplier, as set out or referred to in Schedule 25 (<i>Exit Management</i>);
“Exit Plan”	the plan produced and updated by the Supplier during the Term in accordance with Paragraph 4 of Schedule 25 (<i>Exit Management</i>);
“Expedited Dispute Timetable”	the reduced timetable for the resolution of Disputes set out in Paragraph 3 of Schedule 23 (<i>Dispute Resolution Procedure</i>);
“Expert”	has the meaning given in Schedule 23 (<i>Dispute Resolution Procedure</i>);
“Expert Determination”	the process described in Paragraph 6 of Schedule 23 (<i>Dispute Resolution Procedure</i>);
“Exposure Information (Contracts List)”	means part of the CRP Information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 2 and Annex 1 of Part B of Schedule 26 (<i>Service Continuity Plan and Corporate Resolution Planning</i>);
“Extension Period”	a period of a maximum of three (3) years from the end of the Initial Term;
“Failed Change”	means as set out in Paragraph 5.1 of Part B of Annex 1 of Schedule 3 (<i>Performance Levels</i>);
“Facilities Management Contractor”	means the Other Supplier(s) that provide(s) facility management services to the Authority;
“Field Services”	means the Services as described in Paragraph 2.2 of the Technical Requirements;
“Financial Distress Event”	the occurrence of one or more of the events listed in Paragraph 3.1 of Schedule 18 (<i>Financial Distress</i>);

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Financial Information and Commentary”	means part of the CRP Information requirements set out in accordance with Paragraphs 2 and Annex 3 of Part B of Schedule 26 (<i>Service Continuity Plan and Corporate Resolution Planning</i>);
“Financial Distress Remediation Plan”	a plan setting out how the Supplier will ensure the continued performance and delivery of the Services in accordance with this Contract in the event that a Financial Distress Event occurs. This plan should include what the Authority would need to put in place to ensure performance and delivery of the Services in accordance with this Contract up to and including any Insolvency Event in respect of the relevant FDE Group entity and may refer to the Insolvency Continuity Plan in this regard;
“Financial Model”	has the meaning given in Schedule 19 (<i>Financial Reports and Audit Rights</i>);
“Financial Reports”	has the meaning given in Schedule 19 (<i>Financial Reports and Audit Rights</i>);
“Financial Transparency Objectives”	has the meaning given in Schedule 19 (<i>Financial Reports and Audit Rights</i>);
“First Draft Delivery Date”	the planned date, as stated in the Document Review Plan, by which the Supplier shall submit a draft Documentary Deliverable to the Authority;
“First Extension Period”	a period of one (1) year from the end of the Initial Term;
“FOIA”	the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time, together with any guidance and/or codes of practice issued by the Information Commissioner or any relevant Crown Body in relation to such Act;
“Force Majeure Event”	any event outside the reasonable control of either Party affecting its performance of its obligations under this Contract arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party, including riots, war or armed conflict, acts of terrorism, acts of government, local government or regulatory bodies, fire, flood, storm or earthquake, or other natural disaster but excluding any industrial dispute relating to the Supplier or the Supplier Personnel or any other failure in the Supplier's or a Sub-contractor's supply chain;

"Force Majeure Notice" a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event;

"Former Supplier" has the meaning given in Schedule 28 (*Staff Transfer*);

"Gateway LAN" as described in Paragraph 4.3.1 of the Technical Requirements;

"Gateway Services" has the meaning given in requirement 4.2.1.1 of the Technical Requirements;

"Gateway System" means the Authority Assets of the Authority System which are hosted within the Authority Data Centres and which are or may be used in connection with the provision or receipt of the Gateway Services and/or the Core Network Services;

"Gateway Test System" means Authority Assets of the Gateway System which are or may be used by Other Suppliers, the Authority, Service Recipients and/or the Supplier for the development and testing of the End to End Services;

"General Anti-Abuse Rule" (a) the legislation in Part 5 of the Finance Act 2013; and
(b) any future legislation introduced into Parliament to counteract tax advantages arising from abusive arrangements to avoid national insurance contributions;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“General Change in Law”	a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
“Good Industry Practice”	at any time, the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would be reasonably expected at such time from a leading and expert supplier of services similar to the Services to a customer like the Authority, such supplier seeking to comply with its contractual obligations in full and complying with applicable Laws;
“Goods”	has the meaning given in Clause 9.7 (Supply of Goods);
“Gold Site”	means an Authority Site which is specified as being a Gold Site in the Authority Site List, is resilient and in the reasonable opinion of the Authority has a high level of business criticality;
“Government Security Classifications”	has the meaning given to it at Government Security Classifications - https://www.gov.uk/government/publications/government-security-classifications ;
“Guarantee”	the deed of guarantee in favour of the Authority entered into by the Guarantor as required by the Authority during the Term (which is in the form set out in Schedule 30 (<i>Guarantee</i>)), or any guarantee acceptable to the Authority that replaces it from time to time;
“Guarantor”	the company who the Supplier identifies and who subsequently enters into the Guarantee;
“Halifax Abuse Principle”	the principle explained in the CJEU Case C-255/02 Halifax and others;
“Health and Safety Policy”	the health and safety policy of the Authority and/or other relevant Crown Body as provided to the Supplier on or before the Effective Date and as subsequently provided

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	to the Supplier from time to time except any provision of any such subsequently provided policy that cannot be reasonably reconciled to ensuring compliance with applicable Law regarding health and safety;
“High Level Design” or “HLD”	has the meaning given in requirement 3.2.1.22 of the Technical Requirements;
“HMRC”	HM Revenue & Customs;
“ICT”	means information and communications technology;
“Impact Assessment”	has the meaning given in Part A of Schedule 22 (<i>Change Control Procedure, Service Requests and Projects</i>);
“Implementation Period”	means the period (or periods) from the Effective Date until the relevant Operational Service Commencement Date;
“Implementation Plan”	means the Outline Implementation Plan or (if and when approved by the Authority pursuant to Paragraph 3 of Schedule 13 (<i>Implementation Plan</i>)) the Detailed Implementation Plan as updated in accordance with Paragraph 4 of Schedule 13 (<i>Implementation Plan</i>) from time to time;
“Implementation Services”	means the Services described in the Transition Requirements;
“Implementation Services Commencement Date”	the date on which the Supplier is to commence provision of the first of the Implementation Services, being the Effective Date;
“Incident”	a Service Incident and/or a Security Incident;
“Incident Management System”	means the processes, tools and data used in the ITSM Toolset for the purpose of managing Incidents;
“Indemnified Person”	the Authority, each Service Recipient and each and every person to whom the Authority (or any direct or indirect sub-licensee of the Authority) sub-licenses,

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

assigns or novates any Relevant IPRs or rights in Relevant IPRs in accordance with this Contract;

“Independent Controller”

a party which is Controller of the same Personal Data as the other Party and there is no element of joint control with regards to that Personal Data;

“Information”

all information of whatever nature, however conveyed and in whatever form, including in writing, orally, by demonstration, electronically and in a tangible, visual or machine-readable medium (including CD-ROM, magnetic and digital form);

“Initial Term”

the period of seven (7) years from and including the Effective Date;

“Initial Upload Date”

means the occurrence of an event detailed in Schedule 24 (*Reports and Records Provisions*) Annex 3: (*Records To Upload To Virtual Library*) which requires the Supplier to provide its initial upload of the relevant information to the Virtual Library;

“Insolvency Event”

with respect to any person, means:

- (a) that person suspends, or threatens to suspend, payment of its debts, or is unable to pay its debts as they fall due or admits inability to pay its debts, or:
 - (i) (being a company or a LLP) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986, or
 - (ii) (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986;
- (b) that person commences negotiations with one or more of its creditors (using a voluntary arrangement, scheme of arrangement or otherwise) with a view to rescheduling any of its debts, or

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

makes a proposal for or enters into any compromise or arrangement with one or more of its creditors or takes any step to obtain a moratorium pursuant to Section 1A and Schedule A1 of the Insolvency Act 1986 other than (in the case of a company, a LLP or a partnership) for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;

- (c) another person becomes entitled to appoint a receiver over the assets of that person or a receiver is appointed over the assets of that person;
- (d) a creditor or encumbrancer of that person attaches or takes possession of, or a distress, execution or other such process is levied or enforced on or sued against, the whole or any part of that person's assets and such attachment or process is not discharged within fourteen (14) days;
- (e) that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business;
- (f) where that person is a company, a LLP or a partnership:
 - (i) a petition is presented (which is not dismissed within fourteen (14) days of its service), a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of that person other than for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (ii) an application is made to court, or an order is made, for the appointment of an administrator, or if a notice of intention to appoint an administrator is filed at Court or given or if an administrator is appointed, over that person;
 - (iii) (being a company or a LLP) the holder of a qualifying floating charge over the assets of that person has become entitled to appoint or has appointed an administrative receiver; or
 - (iv) (being a partnership) the holder of an agricultural floating charge over the assets of that person has become entitled to appoint or has appointed an agricultural receiver; or
 - (g) any event occurs, or proceeding is taken, with respect to that person in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned above;
- “Intellectual Property Rights” or “IPRs”**
- (a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information;
 - (b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and
 - (c) all other rights having equivalent or similar effect in any country or jurisdiction;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Intervention Cause”	has the meaning given in Clause 27.1 (Remedial Adviser);
“Intervention Notice”	has the meaning given in Clause 27.1 (Remedial Adviser);
“Intervention Period”	has the meaning given in Clause 27.2(c) (Remedial Adviser);
“Intervention Trigger Event”	(a) any event falling within limb (a), (b), (c), (e), (f) or (g) of the definition of a Supplier Termination Event; (b) a Default by the Supplier that is materially preventing or materially delaying the performance of the Services or any material part of the Services; (c) the Supplier accruing in aggregate 2355 or more Service Points (in terms of the number of points allocated) in any period of 2 months; (d) the Supplier accruing Service Credits which meet or exceed the Service Credit Cap in four or more of the Service Periods in any consecutive 12 month period; and/or (e) the Supplier not Achieving a Key Milestone within seventy-five (75) days of its relevant Milestone Date;
“IP”	means internet protocol;
“IPAM”	means internet protocol address management;
“IPAM Service”	has the meaning given in requirement 5.6.1 of the Technical Requirements;
“IP Address Plan”	as described in requirement 5.4.1.3 of the Technical Requirements;
“IP Completion Day”	has the meaning given to it in the European Union (Withdrawal Agreement) Act 2020;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“IPRs Claim”	any claim against any Indemnified Person of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any Relevant IPRs save for any such claim to the extent that it is caused by any use by or on behalf of that Indemnified Person of any Relevant IPRs, or the use of the Authority Software by or on behalf of the Supplier, in either case in combination with any item not supplied or recommended by the Supplier pursuant to this Contract or for a purpose not reasonably to be inferred from the Services Description or the provisions of this Contract;
“IPv4”	means internet protocol version 4 as defined by the Internet Engineering Task Force;
“IPv6”	means internet protocol version 6 as defined by the Internet Engineering Task Force;
“IT”	means information technology;
“IT Environment”	the Authority System and the Supplier System;
“IT Health Check”	has the meaning given in Schedule 5 (<i>Security Management</i>);
“IT Personnel”	means people who have day to day responsibility for running the Services;
“IT Service Continuity Management Plan” or “ITSCM Plan”	as described in in Schedule 26 (<i>Service Continuity Plan and Corporate Resolution Planning</i>);
“IT Service Continuity Management” or “ITSCM”	means the Process of the same name listed in Paragraph 13.1 of Schedule 4 (<i>Standards</i>);
“IT Service Continuity Plan” or “ITSC Plan”	as described in in Schedule 26 (<i>Service Continuity Plan and Corporate Resolution Planning</i>);
“ITSM Toolset”	the IT service management system operated and provided by the Authority for management of its services, including the

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	Services and services provided by Other Suppliers;
“Joint Controllers”	has the meaning given in Article 26 of the UK GDPR, or EU GDPR, as the context requires;
“Joint Strategic Partnership Board”	the board as described in Schedule 21 (<i>Governance</i>);
“Key Milestone”	has the meaning given in Schedule 15 (<i>Charges and Invoicing</i>);
“Key Performance Indicator”	the key performance indicators set out in Tables 2 and 4 of Part A of Annex 1 of Schedule 3 (<i>Performance Levels</i>);
“Key Personnel”	those persons appointed by the Supplier to fulfil the Key Roles, being the persons listed in Schedule 29 (<i>Key Personnel</i>) against each Key Role as at the Effective Date or as amended from time to time in accordance with Clauses 14.5 and 14.6 (<i>Key Personnel</i>);
“Key Roles”	a role described as a key role in Schedule 29 (<i>Key Personnel</i>) and any additional roles added from time to time in accordance with Clause 14.4 (<i>Key Personnel</i>);
“Key Sub-contract”	each Sub-contract with a Key Sub-contractor;
“Key Sub-contractor”	any Sub-contractor: (a) which, in the opinion of the Authority, performs (or would perform if appointed) a critical role in the provision of all or any part of the Services; and/or (b) with a Sub-contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the aggregate Charges forecast to be payable under this Contract (as set out in the Financial Model);

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Know-How”	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know how relating to the Services but excluding know how already in the other Party’s possession before this Contract;
“Knowledge Base Article(s)” or “Knowledge Article(s)”	means the core set of knowledge resources Authority staff and End Users use;
“Knowledge Management System”	means the processes, tools and data used in the Authority System for the purpose of managing and maintaining knowledge of the Services;
“KPI Failure”	a failure to meet the Target Performance Level in respect of a Key Performance Indicator;
“KPI Service Threshold”	as set out against the relevant Key Performance Indicator in Tables 2 and 4 of Part A of Annex 1 of Schedule 3 (<i>Performance Levels</i>);
“LAN Service”	means the Authority’s Local Area Network service;
“Law”	any law, statute, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, right within the meaning of the European Union (Withdrawal) Act 2018 as amended by European Union (Withdrawal Agreement) Act 2020, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply;
“LED”	Law Enforcement Directive (Directive (EU) 2016/680);
“Licensed Software”	all and any software licensed by or through the Supplier, its Sub-contractors or any third party to the Authority for the purposes of or pursuant to this Contract, including any

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	Supplier Software, Third Party Software and/or any Specially Written Software;
“Licence Management System”	means the processes, tools and data used in the ITSM Toolset for the purpose of recording and maintaining an accurate record of all the software licences used by the Authority in receipt of the Services;
“Losses”	losses, liabilities, damages, costs and expenses (including legal fees on a solicitor/client basis) and disbursements and costs of investigation, litigation, settlement, judgment interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty or otherwise;
“Low Level Design” or “LLD”	has the meaning given in requirement 3.2.1.22 of the Technical Requirements;
“Maintenance Records”	means the records as described in requirement 6.8.6.1 of the Service Management Requirements;
“Maintenance Schedule”	has the meaning set out in Clause 9.4 (<i>Maintenance</i>);
“Major Incident”	as described in Paragraph 3.3 of Part B of Annex 1 of Schedule 3 (<i>Performance Levels</i>);
“Malicious Software”	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
“Managed Agency Agreement”	an agreement between the Authority, the Supplier and the Managed Supplier in substantially the same form as agreed between the Parties and as attached at Part B of Schedule 11 (<i>Third Party Contracts</i>);

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Managed Supplier”	a supplier with whom the Authority has a Transferring Agreement and that enters into a Managed Agency Agreement with the Authority and the Supplier;
“Management Information”	the management information specified in Schedule 3 (<i>Performance Levels</i>), Schedule 15 (<i>Charges and Invoicing</i>) and Schedule 21 (<i>Governance</i>) to be provided by the Supplier to the Authority;
“Master Time Reference” or “MTR”	as described in requirement 5.2.1.1 B of the Technical Requirements;
“Material KPI Failure”	(a) a Serious KPI Failure; (b) a Severe KPI Failure; or (c) a failure by the Supplier to meet a KPI Service Threshold;
“Material PI Failure”	(a) a failure by the Supplier to meet the PI Service Threshold in respect of 25% or more of the Subsidiary Performance Indicators that are measured in that Service Period; and/or (b) a failure by the Supplier to meet the Target Performance Level in respect of 50% or more of the Subsidiary Performance Indicators that are measured in that Service Period;
“Measurement Period”	in relation to a Key Performance Indicator or Subsidiary Performance Indicator, the period over which the Supplier’s performance is measured (for example, a Service Period if measured monthly or a 12 month period if measured annually);
“Milestone”	an event or task described in the Implementation Plan which, if applicable, shall be completed by the relevant Milestone Date;
“Milestone Achievement Certificate”	the certificate to be granted by the Authority when the Supplier has Achieved a Milestone,

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	which shall be in substantially the same form as that set out in Annex 3 of Schedule 14 (<i>Testing Procedures</i>);
“Milestone Adjustment Payment Amount”	in respect of each CPP Milestone the subject of a Milestone Adjustment Payment Notice, an amount determined in accordance with the formula: $A - B$ where: (a) A is an amount equal to the aggregate sum of all Milestone Payments paid to the Supplier in respect of the Milestones (or in the case of Partial Termination, the Milestones for the parts of the Services terminated) relating to that CPP Milestone; and (b) B is an amount equal to the aggregate Allowable Price for the Retained Deliverables relating to that CPP Milestone or, if there are no such Retained Deliverables, zero;
“Milestone Adjustment Payment Notice”	has the meaning given in Clause 32.7 (Payments by the Supplier);
“Milestone Date”	the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved;
“Milestone Payment”	a payment identified in Schedule 15 (<i>Charges and Invoicing</i>) to be made following the issue of a Milestone Achievement Certificate;
“Milestone Retention”	has the meaning given in Schedule 15 (<i>Charges and Invoicing</i>);
“Minor KPI Failure”	shall be as set out against the relevant Key Performance Indicator in Tables 2 and 4 of Part A of Annex 1 of Schedule 3 (<i>Performance Levels</i>);
“MFA”	means multi factor authentication;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Mobilisation Date”	shall have the same meaning as Transitional Services Commencement Date;
“Modern Slavery Helpline”	the modern slavery helpline phone number on 08000 121 700 or the online reporting tool which can be found online at https://www.modernslaveryhelpline.org/ ;
“MoJ ICT Physical Infrastructure Standards”	the standards regarding ICT physical infrastructure as set out within Paragraph 10 of Schedule 4 (<i>Standards</i>);
“MoJO”	means the Ministry of Justice Official;
“Month”	a calendar month and “ monthly ” shall be interpreted accordingly;
“Multi-Party Dispute Resolution Procedure”	has the meaning given in Paragraph 9.1 of Schedule 28 (<i>Staff Transfer</i>) of Schedule 23 (<i>Dispute Resolution Procedure</i>);
“Multi-Party Procedure Initiation Notice”	has the meaning given in Paragraph 9.2 of Schedule 23 (<i>Dispute Resolution Procedure</i>);
“NCSC”	the National Cyber Security Centre or any replacement or successor body carrying out the same function;
“Network Time Protocol” or “NTP”	has the meaning given to it in requirement 5.2.1.1 A of the Technical Requirements;
“Network to Network Interconnect (NNI)”	means the interface that enables peering that establishes connectivity between the Authority, OGDs, Supplier, Other Suppliers or other third-party networks;
“New Releases”	an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;
“Non-Documentary Deliverables”	any Deliverables excluding Documentary Deliverables;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Non-retained Deliverables”	in relation to a CPP Milestone Payment Notice and each CPP Milestone the subject of that CPP Milestone Payment Notice, Deliverables provided to the Authority which relate to the relevant CPP Milestone(s) and which are not Retained Deliverables;
“Non-Transitioned Site”	an Authority Site which is not a Transitioned Site;
“Non-trivial Customer Base”	a significant customer base with respect to the date of first release and the relevant market but excluding Affiliates and other entities related to the licensor;
“Notifiable Default”	shall have the meaning given in Clause 25.1 (Rectification Plan Process);
“NTE”	means CPE which is network termination equipment;
“Occasion of Tax Non-Compliance”	(a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 is found on or after 1 April 2013 to be incorrect as a result of: (i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle; (ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime; and/or (b) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 gives rise on or after 1 April 2013 to a criminal

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

conviction in any jurisdiction for tax related offences which is not spent at the Effective Date or to a civil penalty for fraud or evasion;

“OGDs”	means other government departments;
“Open Book Data”	has the meaning given in Schedule 19 (<i>Financial Reports and Audit Rights</i>);
“Open Source”	computer software that is released on the internet for use by any person, such release usually being made under a recognised open-source licence and stating that it is released as open source;
“Operating Environment”	the Authority System and the Sites;
“Operational Change”	any change in the Supplier's operational procedures which in all respects, when implemented: (a) will not affect the Charges and will not result in any other costs to the Authority; (b) may change the way in which the Services are delivered but will not adversely affect the output of the Services or increase the risks in performing or receiving the Services; (c) will not adversely affect the interfaces or interoperability of the Services with any of the Authority's IT infrastructure; and (d) will not require a change to this Contract;
“Operational Interlock Document”	has the meaning given in requirement 6.7.2.9 of the Service Management Requirements;
“Operational Service Commencement Date”	in relation to an Operational Service, the later of: (a) the date identified in the Implementation Plan upon which the Operational Service is to commence;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) where the Implementation Plan states that the Supplier must have Achieved an ATP Milestone before it can commence the provision of that Operational Service, the date upon which the Supplier Achieves the relevant ATP Milestone; and
- (c) in relation to an Operational Service delivered at an Authority Site, the date on which a Site Transition Certificate is issued in respect of that Authority Site.

“Operational Services”	the services described in the Services Description but excluding those described in the Transition Requirements and Schedule 34 (<i>Transitional Services</i>);
“Optional Services”	the services described as such in Schedule 2 (<i>Services Description</i>) which are to be provided by the Supplier if required by the Authority in accordance with Clause 5.10 (Optional Services);
“Optional Services Implementation Plan”	the implementation plan to effect the Optional Services agreed between the Parties prior to the Effective Date and, if not agreed prior to the Effective Date, to be developed by the Supplier and approved by the Authority;
“Other Supplier”	means any supplier to the Authority (other than the Supplier) which is notified to the Supplier from time to time;
“Other WAN Supplier”	means the subset of Other Suppliers that is subject to management in accordance with Paragraph 6.8.2 of the Service Management Requirements and as notified by the Authority to the Supplier from time to time; typically, these suppliers provide the Authority with licences or maintenance services related to WAN;
“Outline Implementation Plan”	means the outline plan set out at Annex 1 of Schedule 13 (<i>Implementation Plan</i>);

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Outline Project Plan”	has the meaning given in Paragraph 1.1 of Part B of Schedule 22 (<i>Change Control Procedure, Service Requests and Projects</i>);
“PaaS”	means platform as a service;
“PAM”	means privileged access management;
“Parent Undertaking”	has the meaning set out in section 1162 of the Companies Act 2006;
“Partial Termination”	the partial termination of this Contract to the extent that it relates to the provision of any part of the Services as further provided for in Clause 31.2(b) (Termination by the Authority) or 31.3(b) (Termination by the Supplier) or otherwise by mutual agreement by the Parties;
“Parties” and “Party”	have the meanings respectively given on page 1 of this Contract;
“Payment Planner”	has the meaning given in Schedule 15 (<i>Charges and Invoicing</i>);
“Peering Services”	has the meaning given in requirement 4.5.1.1 of the Technical Requirements;
“Performance Failure”	a KPI Failure or a PI Failure;
“Performance Indicators”	the Key Performance Indicators and the Subsidiary Performance Indicators;
“Performance Monitoring Report”	has the meaning given in Schedule 3 (<i>Performance Levels</i>);
“Permitted Maintenance”	has the meaning given in Clause 9.4 (Maintenance);
“Personal Data”	has the meaning given in the UK GDPR or the EU GDPR as the context requires;
“Personal Data Breach”	has the meaning given in the UK GDPR or the EU GDPR as the context requires;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“PI Failure”	means a failure to meet the Target Performance Level in respect of a Subsidiary Performance Indicator;
“PI Service Threshold”	shall be as set out against the relevant Subsidiary Performance Indicator in Tables 3 and 4 in Part A of Annex 1 of Schedule 3 (<i>Performance Levels</i>);
“Planned Approval Date”	means the planned date by which a Documentary Deliverable should achieve Approval, as set out in the Document Review Plan;
“Post Go Live Report”	means a report covering activities completed post the relevant Operational Service Commencement Date and initial period of Early Life Support, which details any risks, issues or defects identified;
“Preceding Services”	has the meaning given in Clause 5.2(b) (Standard of Services);
“Preceding Supplier”	shall have the same meaning as ‘Former Supplier’ (as defined in Schedule 28 (<i>Staff Transfer</i>);
“Prescribed Person”	a legal adviser, an MP, or an appropriate body which a whistle-blower may make a disclosure to as detailed in ‘Whistleblowing: list of prescribed people and bodies’, available online at: https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies , as updated from time to time;
“Primary Fixed Broadband Services”	as described in requirement 3.2.4.3 of the Technical Requirements;
“Problem”	means the cause of one or more Incidents;
“Problem Management”	means the Process of the same name listed in Paragraph 13.1 of Schedule 4 (<i>Standards</i>);

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Problem Management System”	means the processes, tools and data used in the ITSM Toolset for the purpose of Problem Management;
“Process” or “Processes”	an Authority document (unless the context otherwise requires) that describes processes, actions or strategies as they relate to a particular activity identified in Schedule 4 (<i>Standards</i>) but excluding Standards;
“Processor”	has the meaning given to it under the UK GDPR or the EU GDPR as the context requires;
“Processor Personnel”	means all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Sub-processor engaged in the performance of its obligations under this Contract;
“Product and Service Catalogue”	means the product and services catalogue, that details the Catalogue Items that can be ordered by the Authority in accordance with the Service Request procedure in Part B of Schedule 22 (<i>Change Control Procedure, Service Requests and Projects</i>);
“Prohibited Act”	(a) to directly or indirectly offer, promise or give any person working for or engaged by the Authority a financial or other advantage to: (i) induce that person to perform improperly a relevant function or activity; or (ii) reward that person for improper performance of a relevant function or activity; (b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

a relevant function or activity in connection with this Contract;

- (c) an offence:
 - (i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act);
 - (ii) under legislation or common law concerning fraudulent acts; or
 - (iii) defrauding, attempting to defraud or conspiring to defraud the Authority (including offences by the Supplier under Part 3 of the Criminal Finances Act 2017); or
- (d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK;

“Project” means the programme of work undertaken pursuant to a Project Work Order agreed by the Parties in accordance with the procedures set out in Schedule 22 (*Change Control Procedure, Service Requests and Projects*);

“Project Plan” has the meaning given in Paragraph 1.1 of Part B of Schedule 22 (*Change Control Procedure, Service Requests and Projects*);

“Project Proposal” has the meaning given in Paragraph 1.1 of Part B of Schedule 22 (*Change Control Procedure, Service Requests and Projects*);

“Project Request” has the meaning given in Paragraph 1.1 of Part B of Schedule 22 (*Change Control Procedure, Service Requests and Projects*);

“Project Specific IPRs” (a) Intellectual Property Rights in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Contract and updates and

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

amendments of these items including
(but not limited to) database schema;
and/or

- (b) Intellectual Property Rights arising as
a result of the performance of the
Supplier's obligations under this
Contract;

but shall not include the Supplier Background
IPRs or the Specially Written Software;

“Project Test Strategy”

a strategy for the conduct of Testing as
described in Paragraph 4 of Part B of
Schedule 22 (*Change Control Procedure,
Service Requests and Projects*);

“Project Work Order”

means a written document setting out details
of each Project in such form as may be
agreed between the Parties from time to
time, the format of which as at the Effective
Date is as set out in Annex 1 of Part B of
Schedule 22 (*Change Control Procedure,
Service Requests and Projects*);

“Project Work Order Meeting”

has the meaning given in Paragraph 1.1 of
Part B of Schedule 22 (*Change Control
Procedure, Service Requests and Projects*);

“Protective Measures”

means the appropriate technical and
organisational measures designed to ensure
compliance with obligations of the Parties
arising under Data Protection Legislation,
which may include: pseudonymising and
encrypting Personal Data, ensuring
confidentiality, integrity, availability and
resilience of systems and services, ensuring
that availability of and access to Personal
Data can be restored in a timely manner after
an incident, and regularly assessing and
evaluating the effectiveness of the such
measures adopted by it, including those
outlined in Schedule 5 (*Security
Management*);

“PSN Access”

as described in Paragraph 3.3.3 of the
Technical Requirements;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Public Sector Dependent Supplier”	means a supplier where that supplier, or that supplier’s group has Annual Revenue of £50 million or more of which over 50% is generated from UK Public Sector Business;
“Public Services Network (PSN)”	means the network of networks delivered through multiple service providers, as further detailed in the PSN operating model; and described at https://www.gov.uk/government/groups/public-services-network ;
“Publishable Performance Information”	means any of the information in the Performance Monitoring Report as it relates to a Performance Indicator where it is expressed as publishable in the table in Annex 1 which shall not constitute Commercially Sensitive Information;
“Quality Criteria”	the criteria for Approval by the Authority of a Documentary Deliverable, including any criteria set out in the Product Description for that Documentary Deliverable;
“Quality Plans”	has the meaning given in Clause 6.1 (Quality Plans);
“Quarter”	the first three Service Periods and each subsequent three Service Periods (save that the final Quarter shall end on the date of termination or expiry of this Contract);
“Recipient”	has the meaning given in Clause 19.1 (Confidentiality);
“Recall”	a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the IPR rights) that might endanger health or hinder performance;
“Records”	has the meaning given in Paragraph 3.1 of Schedule 24 (<i>Reports and Records Provisions</i>);

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Rectification Plan”

a plan to address the impact of, and prevent the reoccurrence of, a Notifiable Default;

“Rectification Plan Failure”

- (a) the Supplier failing to submit or resubmit a draft Rectification Plan to the Authority within the timescales specified in Clauses 25.4 (Submission of the draft Rectification Plan) or 25.8 (Agreement of the Rectification Plan);
- (b) the Authority, acting reasonably, rejecting a revised draft of the Rectification Plan submitted by the Supplier pursuant to Clause 25.7 (Agreement of the Rectification Plan);
- (c) the Supplier failing to rectify a material Default within the later of:
 - (i) 30 Working Days of a notification made pursuant to Clause 25.2 (Notification); and
 - (ii) where the Parties have agreed a Rectification Plan in respect of that material Default and the Supplier can demonstrate that it is implementing the Rectification Plan in good faith, the date specified in the Rectification Plan by which the Supplier must rectify the material Default;
- (d) a Material KPI Failure re-occurring in respect of the same Key Performance Indicator for the same (or substantially the same) root cause in any of the 3 Measurement Periods subsequent to the Measurement Period in which the initial Material KPI Failure occurred;
- (e) the Supplier not Achieving a Key Milestone by the expiry of the Delay Deduction Period; and/or
- (f) following the successful implementation of a Rectification Plan, the same Notifiable Default recurring within a period of 6 months for the

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

same (or substantially the same) root cause as that of the original Notifiable Default;

“Rectification Plan Process”	the process set out in Clauses 25.4 (Submission of the draft Rectification Plan) to 25.9 (Agreement of the Rectification Plan);
“Registers”	has the meaning given in Schedule 25 (<i>Exit Management</i>);
“Reimbursable Expenses”	has the meaning given in Schedule 15 (<i>Charges and Invoicing</i>);
“Release and Deployment Management”	means the Process of the same name listed in Paragraph 13.1 of Schedule 4 (<i>Standards</i>);
“Release and Deployment Management System”	means the processes, tools and data used in the ITSM Toolset for the purpose of Release and Deployment Management;
“Relevant Authority” or “Relevant Authorities”	means the Authority and the Cabinet Office Markets and Suppliers Team or, where the Supplier is a Strategic Supplier, the Cabinet Office Markets and Suppliers Team;
“Relevant IPRs”	IPRs used to provide the Services or as otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Authority or a third party in the fulfilment of the Supplier’s obligations under this Contract including IPRs in the Specially Written Software, the Supplier Non-COTS Software, the Supplier Non-COTS Background IPRs, the Third Party Non-COTS Software and the Third Party Non-COTS IPRs but excluding any IPRs in the Authority Software, the Authority Background IPRs, the Supplier COTS Software, the Supplier COTS Background IPRs, the Third Party COTS Software and/or the Third Party COTS IPRs;
“Relevant Preceding Services”	has the meaning given in Clause 5.2(b) (Standard of Services);

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Relevant Requirements”	all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State for Justice pursuant to section 9 of the Bribery Act 2010;
“Relevant Tax Authority”	HMRC, or, if applicable, a tax authority in the jurisdiction in which the Supplier is established;
“Relevant Transfer”	a transfer of employment to which the Employment Regulations applies;
“Relief Notice”	has the meaning given in Clause 29.2 (Authority Cause);
“Remedial Adviser”	the person appointed pursuant to Clause 27.2 (Remedial Adviser);
“Remedial Adviser Failure”	has the meaning given in Clause 27.6 (Remedial Adviser);
“Remediation”	means the works required as a pre-requisite to the delivery of Services. For example: (a) additional duct access to a building; (b) additional cable tray capacity; (c) additional cabinet(s) or works within cabinets; (d) additional air conditioning capacity;
“Replacement Services”	any services which are the same as or substantially similar to any of the Services and which the Authority and/or a Service Recipient receives in substitution for any of the Services following the expiry or termination or Partial Termination of this Contract, whether those services are provided by the Authority or a Service Recipient internally and/or by any third party;
“Replacement Supplier”	any third party service provider of Replacement Services appointed by the Authority and/or a Service Recipient from time to time (or where the Authority or a Service Recipient is providing replacement

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	Services for its own account, the Authority or that Service Recipient);
“Request”	has the meaning given in Paragraph 1.1 of Part B of Schedule 22 (<i>Change Control Procedure, Service Requests and Projects</i>);
“Request For Information”	a Request for Information under the FOIA or the EIRs;
“Required Action”	has the meaning given in Clause 28.1(a) (Step-In Rights);
“Retained Deliverables”	has the meaning given in Clause 32.8(b) (Payments by the Supplier);
“Request for Change” or “RFC”	means a request for a Service Change as described in the Change and Evaluation Management Process;
“Residual Risk Statement”	has the meaning given in Paragraph 1 of Part A of Schedule 5 (<i>Security Management</i>);
“RIPE”	Réseaux IP Européens;
“Risk Register”	the register of risks and contingencies that have been factored into any Costs due under this Contract, a copy of which is set out in Annex E of Schedule 15 (<i>Charges and Invoicing</i>);
“Root Cause Analysis”	means an investigation into the underlying or original cause of an Incident or Problem;
“Root Cause Analysis Report”	as described in requirement 6.5.3.5 of the Service Management Requirements;
“SASE”	means secure access service edge;
“SASE Services”	means the SASE services (Optional Service) provided in accordance with Paragraph 6 of the Technical Requirements and Paragraph 6.8.5 of the Service Management Requirements;
“SD-WAN”	means software-defined wide area network;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“SD-WAN Edge Device”	means a Device that provides SD-WAN functionality and enables integration with SASE services, when connected to a network link (or links) such as Access Circuit(s);
“Second Extension Period”	a period of one (1) year from the end of the First Extension Period;
“Security Aspects Letter” or “SAL”	has the meaning given in Paragraph 1 of Part A of Schedule 5 (<i>Security Management</i>);
“Security Assurance”	has the meaning given in Paragraph 1 of Part A of Schedule 5 (<i>Security Management</i>);
“Security Assurance Decision”	has the meaning given in Paragraph 1 of Part A of Schedule 5 (<i>Security Management</i>);
“Security Incident”	has the meaning given in Paragraph 2 of Part B of Annex 1 of Schedule 3 (<i>Performance Levels</i>);
“Security Management Plan”	has the meaning given in Schedule 5 (<i>Security Management</i>);
“Serious KPI Failure”	shall be as set out against the relevant Key Performance Indicator in Tables 2 and 4 of Part A of Annex 1 of Schedule 3 (<i>Performance Levels</i>);
“Service Assets”	all assets and rights used by the Supplier to provide the Services in accordance with this Contract including Assets and Authority Assets;
“Service Asset and Configuration Management”	means the Process of the same name listed in Paragraph 13.1 of Schedule 4 (<i>Standards</i>);
“Service Asset and Configuration Management System” or “SACM”	means the processes, tools and data used in the ITSM Toolset for the purposes of managing Service Assets and Configuration Items;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Service Change”	means any change to the Authority System or Supplier System as described in the Change and Evaluation Management Process;
“Service Charges”	the periodic payments made in accordance with Schedule 15 (<i>Charges and Invoicing</i>) in respect of the supply of the Operational Services, as set out in Paragraph 3 of Part A of Schedule 15 (<i>Charges and Invoicing</i>);
“Service Continuity Plan”	any plan prepared pursuant to Paragraph 2 of Schedule 26 (<i>Service Continuity Plan and Corporate Resolution Planning</i>) as may be amended from time to time;
“Service Continuity Services”	the ITSC, disaster recovery and insolvency continuity services set out in Schedule 26 (<i>Service Continuity Plan and Corporate Resolution Planning</i>);
“Service Credit Cap”	(a) for each Service Period falling within the period of 12 months commencing on the first Operational Service Commencement Date to occur after the Effective Date, [REDACTED] and [REDACTED]; (b) for each Service Period falling within the remainder of the Term, [REDACTED];
“Service Credits”	credits payable by the Supplier due to the occurrence of 1 or more KPI Failures, calculated in accordance with Paragraph 3 of Part C of Schedule 15 (<i>Charges and Invoicing</i>);
“Service Design Package”	has the meaning given in requirement 7.2.1.2 of the Transition Requirements;
“Service Hours”	has the meaning given in Schedule 3 (<i>Performance Levels</i>);
“Service Incident”	has the meaning given in Schedule 3 (<i>Performance Levels</i>);

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Service Level Management System”	means the processes, tools and data used in the ITSM Toolset for the purposes of recording and maintaining the Target Performance Levels and attainment against the Performance Indicators;
“Service Management Requirements”	means the requirements as described in Annex B (WAN Service Management Requirements) to Schedule 2 (<i>Services Description</i>);
“Service Manager”	means a member of the Supplier staff, who shall be a member of the Key Personnel, nominated by the Supplier and approved by the Authority, responsible for managing the delivery of the Services;
“Service Owner”	means a member of the Authority’s staff appointed by the Authority to perform the function of overall management of the Authority's services;
“Service Period”	a calendar month, save that: (a) the first service period for Operational Services shall begin on the first Operational Service Commencement Date and shall expire at the end of the calendar month in which the first Operational Service Commencement Date falls; (b) the first service period for the Transitional Services shall begin on the Transitional Services Commencement Date and shall expire at the end of the calendar month in which the Transitional Services Commencement Date falls; and (c) the final service period shall commence on the first day of the calendar month in which the Term expires or terminates and shall end on the expiry or termination of the Term;
“Service Points”	in relation to a KPI Failure, the points that are set out against the relevant Key Performance Indicator in the sixth column of table 2 in Part A of Annex 1 (<i>Key Performance Indicators</i>)

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	<i>and Subsidiary Performance Indicators) of Schedule 3 (Performance Levels);</i>
“Service Portfolio”	shall have the meaning given to it in ITIL in accordance with Paragraph 1.3.13 of this Schedule;
“Service Portfolio Management”	means the Process of the same name listed in Paragraph 13.1 of Schedule 4 (<i>Standards</i>);
“Service Portfolio Management System”	means the processes, tools and data used in the ITSM Toolset for the purpose of Service Portfolio Management;
“Service Recipient”	has the meaning given in Paragraph 2.1 of Schedule 33 (<i>Service Recipients</i>);
“Service Readiness Reviews”	means the review meetings used to measure the readiness of the Services before they can Achieve service acceptance;
“Service Request”	has the meaning given in Paragraph 1.1 of Part B of Schedule 22 (<i>Change Control Procedure, Service Requests and Projects</i>);
“Services”	any and all of the services to be provided by the Supplier under this Contract, including those set out in Schedule 2 (<i>Services Description</i>) and Schedule 34 (<i>Transitional Services</i>);
“Services Description”	the services description set out in Schedule 2 (<i>Services Description</i>) and Schedule 34 (<i>Transitional Services</i>);
“Service Transfer Date”	has the meaning given in Schedule 28 (<i>Staff Transfer</i>);
“Service Validation and Testing”	shall have the meaning given to it in ITIL in accordance with Paragraph 1.3.13 of this Schedule;
“Severe KPI Failure”	shall be as set out against the relevant Key Performance Indicator in Tables 1 and 2 of Part A of Annex 1 of Schedule 3 (<i>Performance Levels</i>);

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Silver Site”	means an Authority Site which is specified as being a Silver Site in the Authority Site List, is resilient and in the reasonable opinion of the Authority has a medium level of business criticality;
“SIM”	means subscriber identity module;
“Single Point of Contact” or “SPoC”	means the individual, who is the single point of contact for the relevant activity;
“Site Architecture”	means the to-be state architecture for the Authority's sites as described in Paragraph 3.4 of the Technical Requirements;
“Site Types”	refers to the Authority Site classification as included in the Authority Site List;
“Site Transition Certificate”	the certificate to be granted by the Authority when the Supplier has satisfactorily demonstrated to the Authority that an Authority Site is ready to transition to the Operational Services, which certificate shall be in substantially the same form as that set out in Annex 5 of Schedule 14 (<i>Testing Procedures</i>);
“Site(s)”	any premises (including the Authority Premises, the Supplier's premises or third party premises): (a) from, to or at which: (i) the Services are (or are to be) provided; or (ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or (b) where: (i) any part of the Supplier System is situated; or (ii) any physical interface with the Authority System takes place;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“SME”	an enterprise falling within the category of micro, small and medium-sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises;
“Social Value”	the additional social benefits that can be achieved in the delivery of the Contract, set out in the Authority Requirements;
“Social Value Delivery Plan”	as defined at Paragraph 3.1 of Annex D (Social Value Requirements) to Schedule 2 (<i>Services Description</i>);
“Social Value PI”	The Social Value performance indicators set out in Table 3 of Part A of Annex 1 of Schedule 3 (<i>Performance Levels</i>);
“Software”	Specially Written Software, Supplier Software and Third Party Software;
“Software Supporting Materials”	has the meaning given in Paragraph 2.1(a) of Schedule 32 (<i>Intellectual Property Rights</i>) (Specially Written Software and Project Specific IPRs);
“Solution Design”	has the meaning given in requirement 7.2.1.3 of the Transition Requirements;
“Source Code”	computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;
“Specially Written Software”	any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to Supplier Software or Third Party Software

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	created specifically for the purposes of this Contract;
“Specific Change in Law”	a Change in Law that relates specifically to the business of the Authority and which would not affect a Comparable Supply;
“SSL VPN”	means secure socket layer virtual private network;
“Staffing Information”	has the meaning given in Schedule 28 (<i>Staff Transfer</i>);
“Standards”	the standards, policies and/or procedures identified in Schedule 4 (<i>Standards</i>);
“Standards Hub”	means the Government’s open and transparent Standards adoption process as documented at http://standards.data.gov.uk/ ;
“Step-In Notice”	has the meaning given in Clause 28.1 (Step-In Rights);
“Step-In Trigger Event”	(a) any event falling within the definition of a Supplier Termination Event; (b) a Default by the Supplier that is materially preventing or materially delaying the performance of the Services or any material part of the Services; (c) the Authority considers that the circumstances constitute an emergency despite the Supplier not being in breach of its obligations under this Contract; (d) the Authority being advised by a regulatory body that the exercise by the Authority of its rights under Clause 28 (Step-In Rights) is necessary; (e) the existence of a serious risk to the health or safety of persons, property or the environment in connection with the Services; and/or

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	(f) a need by the Authority to take action to discharge a statutory duty;
“Step-Out Date”	has the meaning given in Clause 28.5(b) (Step-In Rights);
“Step-Out Notice”	has the meaning given in Clause 28.5 (Step-In Rights);
“Step-Out Plan”	has the meaning given in Clause 28.6 (Step-In Rights);
“Strategic Supplier”	means those suppliers to government listed at https://www.gov.uk/government/publications/strategic-suppliers ;
“Sub-contract”	any contract or agreement (or proposed contract or agreement) between the Supplier (or a Sub-contractor) and any third party whereby that third party agrees to provide to the Supplier (or the Sub-contractor) all or any part of the Services or facilities or services which are material for the provision of the Services or any part thereof or necessary for the management, direction or control of the Services or any part thereof;
“Sub-contractor”	any third party with whom: (a) the Supplier enters into a Sub-contract; or (b) a third party under (a) above enters into a Sub-contract, or the servants or agents of that third party;
“Sub-processor”	any third party appointed to process Personal Data on behalf of the Processor related to this Contract;
“Subsidiary Performance Indicator”	the performance indicators set out in Table 3 of Part A of Annex 1 of Schedule 3 (<i>Performance Levels</i>);
“Subsidiary Undertaking”	has the meaning set out in section 1162 of the Companies Act 2006;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Successor Body”	has the meaning given in Clause 34.4 (Assignment and Novation);
“Supplier Background IPRs”	(a) Intellectual Property Rights owned by the Supplier before the Effective Date, for example those subsisting in the Supplier's standard development tools, program components or standard code used in computer programming or in physical or electronic media containing the Supplier's Know-How or generic business methodologies; and/or (b) Intellectual Property Rights created by the Supplier independently of this Contract, which in each case is or will be used before or during the Term for designing, testing implementing or providing the Services but excluding Intellectual Property Rights owned by the Supplier subsisting in the Supplier Software;
“Supplier COTS Background IPRs”	any embodiments of Supplier Background IPRs that: (a) the Supplier makes generally available commercially prior to the date of this Contract (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price; and (b) has a Non-trivial Customer Base;
“Supplier COTS Software”	Supplier Software (including open source software) that: (a) the Supplier makes generally available commercially prior to the date of this Contract (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price; and

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	(b) has a Non-trivial Customer Base;
“Supplier Equipment”	the hardware, computer and telecoms devices and equipment used by the Supplier or its Sub-contractors (but not in scope of the Authority System or hired, leased or loaned from the Authority) for the provision of the Services;
“Supplier Group”	means the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings;
“Supplier Non-COTS Background IPRs”	any embodiments of Supplier Background IPRs that have been delivered by the Supplier to the Authority and that are not Supplier COTS Background IPRs;
“Supplier Non-COTS Software”	Supplier Software that is not Supplier COTS Software;
“Supplier Non-Performance”	has the meaning given in Clause 29.1 (Authority Cause);
“Supplier Review Board”	as described in Schedule 21 (<i>Governance</i>);
“Supplier Personnel”	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Sub-contractor engaged in the performance of the Supplier’s obligations under this Contract;
“Supplier Profit”	has the meaning given in Schedule 15 (<i>Charges and Invoicing</i>);
“Supplier Profit Margin”	has the meaning given in Schedule 15 (<i>Charges and Invoicing</i>);
“Supplier Representative”	the representative appointed by the Supplier pursuant to Clause 11.3 (Representatives);
“Supplier Software”	software which is proprietary to the Supplier (or an Affiliate of the Supplier) and which is or will be used by the Supplier for the purposes of providing the Services, including

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	the software specified as such in Schedule 12 (<i>Software</i>);
“Supplier Solution”	the Supplier's solution for the Services set out in Schedule 8 (<i>Supplier Solution</i>) including any Annexes of that Schedule;
“Supplier System”	the information and communications technology system used by the Supplier in implementing and performing the Services including the Software, the Supplier Equipment, configuration, monitoring and management utilities, calibration and testing tools and related cabling (but excluding the Authority System);
“Supplier Termination Event”	(a) the Supplier's level of performance constituting a Critical Performance Failure in accordance with Clause 7.6; (b) the Supplier committing a material Default which is irremediable; (c) as a result of the Supplier's Default, the Authority incurring Losses in any Contract Year which exceed 80% of the value of the aggregate annual liability cap for that Contract Year as set out in Clause 23.4(d) (Financial and other Limits); (d) a Remedial Adviser Failure; (e) a Rectification Plan Failure; (f) where a right of termination is expressly reserved in this Contract, including pursuant to: (i) Clause 17 (IPRs Indemnity); (ii) Clause 33 (Compliance); (iii) Clause 37.6(b) (Prevention of Fraud and Bribery); and/or (iv) Paragraph 6 of Schedule 18 (<i>Financial Distress</i>); (v) Paragraph 3 of Part B to Schedule 26 (<i>Service</i>

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Continuity Plan and Corporate Resolution Planning);

- (g) the representation and warranty given by the Supplier pursuant to Clauses 3.2(h) or 3.2(i) (*Warranties*) being materially untrue or misleading;
- (h) the Supplier committing a material Default under Clause 10.10 (Promoting Tax Compliance) or failing to provide details of steps being taken and mitigating factors pursuant to Clause 10.10 (Promoting Tax Compliance) which in the reasonable opinion of the Authority are acceptable;
- (i) the Supplier committing a material Default under any of the following:
 - (i) Clause 5.5(j) (*Services*);
 - (ii) Clause 21 (Protection of Personal Data);
 - (iii) Clause 20 (Transparency and Freedom of Information);
 - (iv) Clause 19 (Confidentiality); and
 - (v) Clause 33 (Compliance);
 - (vi) in respect of any security requirements or Cyber Essentials obligations set out in Schedule 2 (*Services Description*), Schedule 5 (*Security Management*) or the Baseline Security Requirements;
 - (vii) in respect of any requirements set out in Schedule 32 (*Intellectual Property Rights*); and/or
 - (viii) in respect of any requirements set out in Schedule 28 (*Staff Transfer*);

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (j) any failure by the Supplier to implement the changes set out in a Benchmark Report as referred to in Paragraph 5.9 of Schedule 17 (*Benchmarking*);
- (k) an Insolvency Event occurring in respect of the Supplier;
- (l) not used;
- (m) a change of Control of the Supplier unless:
 - (i) the Authority has given its prior written consent to the particular change of Control, which subsequently takes place as proposed; or
 - (ii) the Authority has not served its notice of objection within 6 months of the later of the date on which the change of Control took place or the date on which the Authority was given notice of the change of Control;
- (n) a change of Control of a Key Sub-contractor unless, within 6 months of being notified by the Authority that it objects to such change of Control, the Supplier terminates the relevant Key Sub-contract and replaces it with a comparable Key Sub-contract which is approved by the Authority pursuant to Clause 15.10 (*Appointment of Key Sub-contractors*);
- (o) any failure by the Supplier to enter into or to comply with an Admission Agreement under Part D of Schedule 28 (*Staff Transfer*);
- (p) the Authority has become aware that the Supplier should have been excluded under Regulation 57(1) or (2) of the Public Contracts Regulations 2015 from the

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

procurement procedure leading to the award of this Contract;

- (q) a failure by the Supplier to comply in the performance of the Services with legal obligations in the fields of environmental, social or labour law; or
- (r) in relation to Schedule 5 (*Security Management*):
 - (i) the Authority has issued two rejection notices in respect of the Security Management Plan under Paragraph 6.9;
 - (ii) the Supplier fails to implement a change required by the Required Changes Register in accordance with the timescales set out in the Required Changes Register; and/or
 - (iii) the Supplier fails to comply with the Incident Management Process;
- (s) the Supplier is in material Default of any Joint Controller Agreement relating to the Contract;
- (t) a Default that occurs and continues to occur on one or more occasions within 6 Months following the Authority serving a warning notice on the Supplier that it may terminate for persistent breach of the Contract; or
- (u) the Supplier or its Affiliates embarrass or bring the Authority into disrepute or diminish the public trust in them.

“Supply Chain Map”

means details of (i) the Supplier, (ii) all Sub-contractors and (iii) any other entity that the Supplier is aware is in its supply chain that is not a Sub-contractor, setting out at least:

- (a) the name, registered office and company registration number of each entity in the supply chain;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	(b) the function of each entity in the supply chain; and the location of any premises at which an entity in the supply chain carries out a function in the supply chain;
“Supply Chain Transparency Report”	means the report provided by the Supplier to the Authority in the form set out in Annex 4 of Schedule 24 (<i>Reports and Records Provisions</i>);
“Target Performance Level”	the minimum level of performance for a Performance Indicator which is required by the Authority, as set out against the relevant Performance Indicator in the tables in Annex 1 of Schedule 3 (<i>Performance Levels</i>);
“Technical Requirements”	means the requirements as described in Annex A (WAN Technical Requirements) to Schedule 2 (<i>Services Description</i>);
“Term”	the period commencing on the Effective Date and ending on the expiry of the Initial Term or any Extension Period or on earlier termination of this Contract;
“Termination Assistance Notice”	has the meaning given in Paragraph 5 of Schedule 25 (<i>Exit Management</i>);
“Termination Assistance Period”	in relation to a Termination Assistance Notice, the period specified in the Termination Assistance Notice for which the Supplier is required to provide the Termination Services as such period may be extended pursuant to Paragraph 5.2 of Schedule 25 (<i>Exit Management</i>);
“Termination Date”	the date set out in a Termination Notice on which this Contract (or a part of it as the case may be) is to terminate;
“Termination Notice”	a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate this Contract (or any part thereof) on a specified

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	date and setting out the grounds for termination;
“Termination Payment”	the payment determined in accordance with Schedule 16 (<i>Payments on Termination</i>);
“Termination Services”	the services and activities to be performed by the Supplier pursuant to the Exit Plan, including those activities listed in Annex 1 of Schedule 25 (<i>Exit Management</i>), and any other services required pursuant to the Termination Assistance Notice;
“Test Issues”	has the meaning given in Schedule 14 (<i>Testing Procedures</i>);
“Test Manager”	means the Single Point of Contact, who shall be a member of the Key Personnel, nominated by the Supplier and approved by the Authority, who is responsible for Service Validation and Testing;
“Tests” and “Testing”	any tests required to be carried out under this Contract, as further described in Schedule 14 (<i>Testing Procedures</i>) and “Tested” shall be construed accordingly;
“Test Plan”	has the meaning given in Schedule 14 (<i>Testing Procedures</i>);
“Test Schedule”	means a list of activities and their associated timescale for the testing of the ITSC Plans;
“Test Strategy”	has the meaning given in Schedule 14 (<i>Testing Procedures</i>);
“Test Success Criteria”	has the meaning given in Schedule 14 (<i>Testing Procedures</i>);
“Third Extension Period”	a period of one (1) year from the end of the Second Extension Period;
“Third Party Auditor”	an independent third party auditor as appointed by the Authority from time to time to confirm the completeness and accuracy of information uploaded to the Virtual Library in accordance with the requirements outlined in

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Schedule 24 (*Reports and Records Provisions*);

“Third Party Beneficiary” has the meaning given in Clause 41.1 (Third Party Rights);

“Third Party Contracts” has the meaning given in Schedule 16 (*Payments on Termination*);

“Third Party COTS IPRs” Third Party IPRs that:

- (a) the supplier makes generally available commercially prior to the date of this Contract (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the supplier save as to price; and
- (b) has a Non-trivial Customer Base;

“Third Party COTS Software” Third Party Software (including open source software) that:

- (a) the supplier makes generally available commercially prior to the date of this Contract (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the supplier save as to price; and
- (b) has a Non-trivial Customer base;

“Third Party IPRs” Intellectual Property Rights owned by a third party, but excluding Intellectual Property Rights owned by the third party subsisting in any Third Party Software, which in any case is, will be or is proposed to be used by the Supplier for the purposes of providing the Services;

“Third Party Non-COTS IPRs” Third Party IPRs that are not Third Party COTS IPRs;

“Third Party Non-COTS Software” Third Party Software that is not Third Party COTS Software;

“Third Party Provisions” has the meaning given in Clause 41.1 (Third Party Rights);

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Third Party Software”	software which is proprietary to any third party (other than an Affiliate of the Supplier) or any Open Source Software which in any case is, will be or is proposed to be used by the Supplier for the purposes of providing the Services, including the software specified as such in Schedule 12 (<i>Software</i>);
“Transferable Assets”	has the meaning given in Schedule 25 (<i>Exit Management</i>);
“Transferring Assets”	has the meaning given in Paragraph 6.2(a) of Schedule 25 (<i>Exit Management</i>);
“Transferring Agreements”	the contracts listed in Part B of Schedule 11 (<i>Third Party Contracts</i>) which are to be transferred by the Authority to the Supplier with effect from the applicable Agreed Transfer Date;
“Transferring Authority Employees”	has the meaning given in Schedule 28 (<i>Staff Transfer</i>);
“Transferring Former Supplier Employees”	has the meaning given in Schedule 28 (<i>Staff Transfer</i>);
“Transferring Supplier Employees”	has the meaning given in Schedule 28 (<i>Staff Transfer</i>);
“Transition”	has the meaning given in requirement 7.1.1.1 of the Transition Requirements;
“Transition / Exit Board”	the transition / exit board as described in Schedule 21 (<i>Governance</i>);
“Transition Framework”	means the Process of the same name listed in Paragraph 13.1 of Schedule 4 (<i>Standards</i>);
“Transition Lead”	has the meaning given in requirement 7.1.1.4 of the Transition Requirements;
“Transition Planning and Support System”	means the processes, tools and data used in the ITSM Toolset for the purpose of planning and managing the transition of the Services to the live environment;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Transition Principles”	has the meaning given in Paragraph 3.3.2 of Schedule 2 (<i>Services Description</i>);
“Transition Requirements”	means the requirements as described in Annex C (WAN Transition Requirements) to Schedule 2 (<i>Services Description</i>) and Schedule 34 (<i>Transitional Services</i>);
“Transitional Services”	as described in Schedule 34 (<i>Transitional Services</i>);
“Transitional Services Commencement Date”	the date on which the Supplier is to commence provision of the Transitional Services, being the later of: (a) the date identified in the Implementation Plan upon which the Transitional Services mobilisation is complete and the Transitional Services are to commence; and (b) the date upon which the Supplier Achieves Milestone 1b;
“Transitioned Site”	an Authority Site in respect of which the Authority has issued a Site Transition Certificate;
“Transparency Information”	has the meaning given in Clause 20.1 (Transparency and Freedom of Information);
“Transparency Reports”	has the meaning given in Schedule 24 (<i>Reports and Records Provisions</i>);
“Transport Services”	has the meaning given in requirement 3.2.1.1 of the Technical Requirements;
“UK”	the United Kingdom;
“UKAS”	means United Kingdom Accreditation Service;
“UK GDPR”	has the meaning as set out in section 3(10) of the DPA 2018, supplemented by section 205(4) of the DPA 2018;

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“UK Public Sector Business”	means any goods, service or works provision to UK public sector bodies, including Crown Bodies and their arm's length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police, fire and rescue, education bodies and devolved administrations;
“Unacceptable KPI Failure”	means the Supplier failing to achieve the KPI Service Threshold in respect of more than 50% of the Key Performance Indicators that are measured in that Service Period;
“Unconnected Sub-contract”	any contract or agreement which is not a Sub-contract and is between the Supplier and a third party (which is not an Affiliate of the Supplier) and is a qualifying contract under regulation 6 of The Reporting on Payment Practices and Performance Regulations 2017;
“Unconnected Sub-contractor”	any third party with whom the Supplier enters into an Unconnected Sub-contract;
“Unrecovered Payment”	has the meaning given in Schedule 16 (<i>Payments on Termination</i>);
“Updates”	in relation to any Software and/or any Deliverable means a version of such item which has been produced primarily to overcome Defects in, or to improve the operation of, that item;
“Update Requirement”	means the occurrence of an event detailed in Schedule 24 (<i>Reports and Records Provisions</i>) (Annex 3: <i>Records To Upload To Virtual Library</i>) which requires the Supplier to update the relevant information hosted on the Virtual Library;
“Upgrades”	any patch, New Release or upgrade of Software and/or a Deliverable, including standard upgrades, product enhancements, and any modifications, but excluding any Update which the Supplier or a third party software supplier (or any Affiliate of the

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	Supplier or any third party) releases during the Term;
“URL”	means uniform resource locator;
“Valid”	in respect of an Assurance, has the meaning given in Paragraph 2.7 of Part B to Schedule 26 (<i>Service Continuity Plan and Corporate Resolution Planning</i>);
“VAT”	value added tax as provided for in the Value Added Tax Act 1994;
“VCSE”	means a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives;
“Virtual Library”	means the data repository hosted by the Authority containing the information about this Contract and the Services provided under it in accordance with Schedule 24 (<i>Reports and Records Provisions</i>);
“ViSOR”	means the Violent Sex Offenders Register application hosted by the police;
“VPN”	means virtual private network;
“WAN”	means Wide Area Network;
“WAN Connectivity”	means all Services described in Paragraph 3 of the Technical Requirements;
“WAN Cutover Approach”	has the meaning given in requirement 7.2.1.17 of the Transition Requirements;
“WAN Service Management Requirements”	means the requirements as described in Paragraph 6.8 of the Service Management Requirements;
“WAN Services Provisioning Process”	has the meaning given in requirement 7.1.1.7 of the Transition Requirements;
“Wider Information Management System” or “WIMS”	has the meaning given in Paragraph 1 of Part A of Schedule 5 (<i>Security Management</i>);

SCHEDULE 1 (DEFINITIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Workaround”	means reducing or eliminating the impact of an Incident or Problem for which a full resolution is not yet available;
“Working Day”	any day other than a Saturday, Sunday or public holiday in England and Wales.

SCHEDULE 2 (Services Description)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 2

SERVICES DESCRIPTION

SCHEDULE 2 (Services Description)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 2 (Services Description)

1 DEFINITIONS

- 1.1 In this Schedule 2, unless the context otherwise requires, capitalised expressions shall have the meanings set out in Schedule 1 (Definitions).

2 INTRODUCTION

- 2.1 The Authority's network services (including Operational Services) are integral to the Authority's ability to deliver its services to the public. This Contract is one of a number of agreements supporting delivery of the End to End Services and to deliver the following objectives:

- Align with the Authority's wider business and technology strategies;
- Shape and future-proof the Authority's technology infrastructure and services;
- Ensure technology service contracts are fit for purpose and value for money;
- Maintain business continuity for end users; and
- Create flexibility to suit the changing needs across the business.

- 2.2 This Schedule 2 sets out the Authority's requirements in relation to each of the following aspects of the Services:

- (a) Annex A (WAN Technical Requirements);
- (b) Annex B (WAN Service Management Requirements);
- (c) Annex C (WAN Transition Requirements); and
- (d) Annex D (WAN Social Value Requirements).

3 SERVICES DESCRIPTION

3.1 Technical Requirements

- 3.1.1 The technical services to be provided by the Supplier contain four key service groupings:

- a) Field Services – installing, moving and decommissioning Devices at/from Authority Sites (as summarised in Paragraph 3.1.4);
- b) WAN Connectivity – provision of secure connectivity to corporate services from all Authority Sites (as summarised in Paragraph 3.1.5 below);

SCHEDULE 2 (Services Description)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- c) Gateway Services – provision of secure access to other network domains, cross-government services, and the internet (as summarised in Paragraph 3.1.6 below); and
- d) Core Network Services – provision of services necessary for the delivery of the end-to-end network services (as summarised in Paragraph 3.1.7 below).

3.1.2 There is a fifth service grouping, SASE Services, which is one of the Optional Services which the Authority may require the Supplier to provide in accordance with Clauses 5.10 to 5.12.

3.1.3 Figure 1 below illustrates the structure of the Technical Requirements.

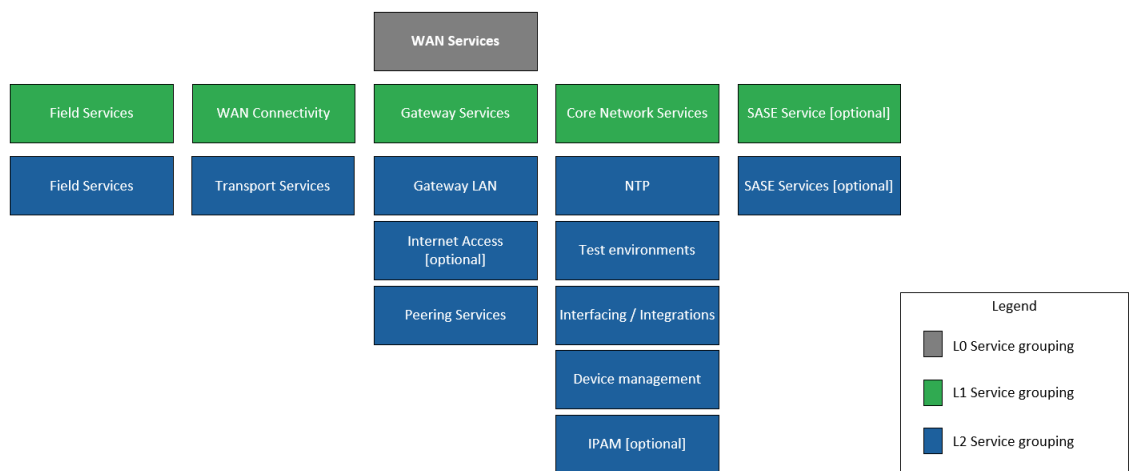


Figure 1: Technical Requirements taxonomy

3.1.4 Field Services are comprised of:

- a) Installation of Devices (including SD-WAN Edge Devices, any interface cards, and intelligent power strips) at the Authority Sites;
- b) Decommissioning Devices, including controlled disconnection from the Authority System, applying security controls to Authority Data as required, removal from rack and removal from the Authority Site; and
- c) Relocating Devices from one Authority Site to another.

3.1.5 WAN Connectivity is comprised of:

- a) Provision of dedicated internet access (DIA), enterprise-grade fixed broadband and mobile broadband services (excluding airtime) at the Authority Sites; and

SCHEDULE 2 (Services Description)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- b) Relevant Supplier Equipment installed at the Authority Sites and managed by the Supplier as CPE;

3.1.6 Gateway Services are comprised of:

- a) Services that facilitate the transfer of data between different network segments or Devices, enabling the flow of traffic between physical and logical networks including through and to the Authority Data Centres ("DC Transit LAN");
- b) Services that enable seamless secure communication and data transfer between the Authority Data Centres ("DC Interconnect");
- c) The remote access solution utilised by the Authority to access, over the PSN, the ViSOR application hosted by the Police;
- d) A secure, resilient network-to-network interconnect gateway; and
- e) Monitoring, management and maintenance of the Authority Assets for the above Services.

3.1.7 Core Network Services are comprised of:

- a) Provision of a secure and authenticated master time reference service;
- b) A centralised privileged access management (PAM) service which performs authentication, authorisation and accounting (AAA) of access to the Devices;
- c) Maintenance and management of the components that comprise the Gateway Test System; and
- d) Integration with Authority's IPAM and DHCP services and interfacing with the Authority's DNS.

3.1.8 The SASE Services (Optional Services) are comprised of the provision of service subscriptions (e.g. SaaS; support subscriptions) and professional services for a specific vendor's SASE solution.

3.1.9 The Technical Requirements are detailed in Annex A (WAN Technical Requirements).

3.2 Service Management Requirements**3.2.1 The Service Management Requirements comprise:**

- a) The standard Service Management Requirements, which support the Authority's standard service operations' approach to managing technology services; and
- b) The WAN Service Management Requirements, which are specific to this Contract.

SCHEDULE 2 (Services Description)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

3.2.2 The aim is to ensure that the components of the Operational Services are delivered and managed as a coherent end-to-end service.

3.2.3 To deliver the above for the Operational Services, the Authority requires the Supplier to:

- a) Interface with the Authority's Service Management framework;
- b) Support the integration and automation of key Service Management processes where appropriate;
- c) Operate and manage the tools / systems to provide Service Management in a cost effective and efficient manner;
- d) Operate and manage tools / systems that provide the Authority with holistic and real-time visibility of the end-to-end services provided; and
- e) Adopt pro-active monitoring and management of the services, identifying, raising, and working collaboratively with the Authority in the resolution of issues / incidents.

3.2.4 The Service Management Requirements are detailed in Annex B (WAN Service Management Requirements).

3.3 Transition Requirements

3.3.1 The Transition Requirements set out the Implementation Services including the processes and conditions for effective transition from the Preceding Services and Transitional Services to the Operational Services.

3.3.2 The Parties acknowledge the following principles (the "**Transition Principles**") as essential to the success of Transition, and the Supplier shall follow the Transition Principles throughout the planning and execution of the Implementation Services:

- A. **Deliver benefits early.** The Authority wishes to enjoy the benefits of the Operational Services as early as possible. During implementation of Operational Services, activities which will bring the greatest benefit should be prioritised.
- B. **Minimise disruption.** Transition should be 'invisible' to service users of the Authority's and the Service Recipients' services, and to most of the End Users. The Implementation Services should be planned and managed to ensure that disruption is minimal. Effectively planned, optimised roll-out is key to this principle.
- C. **Maintain security.** Control risks to security of the Authority Data throughout all aspects of the Implementation Services.
- D. **Collaborate effectively.** Effective collaboration across the Authority's supply chain is crucial – including collaboration between the Supplier and the Preceding Suppliers, Other Suppliers and their relevant sub-contractors.

SCHEDULE 2 (Services Description)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- E. **Deliver on time.** The Implementation Services and Implementation Plan must be controlled and managed so that Operational Service Commencement Dates are Achieved on or ahead of schedule.
- F. **Transfer, retain and re-use knowledge.** The Authority is committed to ensuring it fully uses and reuses the knowledge that it creates and that is created on its behalf. The Preceding Suppliers' and the Supplier's understanding and documentation of the Authority System, Preceding Services and Transitional Services must be transferred, preserved and used effectively for delivery of the Services.

3.3.3 The Transition Requirements shall also apply to the implementation of Optional Services, to the extent that the requirements are applicable to the relevant Optional Services.

3.3.4 The Transition Requirements also set out the Supplier's responsibilities for managing the Transitional Services.

3.3.5 The Transition Requirements are detailed in Annex C (WAN Transition Requirements).

3.4 Social Value Requirements

3.4.1 The Social Value Requirements detail the additional social, economic and environmental benefits to be delivered by the Supplier in line with the Public Services (Social Value) Act 2012, PPN 06/20, and the Authority policies and practices. They align to two key themes:

- a) Creating employment and training opportunities particularly for those who face barriers to employment and/or who are located in deprived areas and/or can be supported to avoid reoffending and, for people in industries with known skills shortages or in high growth sectors; and
- b) Delivering additional environmental benefits in the performance of the contract including working towards net zero greenhouse gas emissions.

3.4.2 The Social Value Requirements are detailed in Annex D (WAN Social Value Requirements).

3.5 Optional Services

3.5.1 Within the scope of the Services are a number of Optional Services, which are identified as being Optional Services in the heading of the relevant section of the Technical Requirements and the Service Management Requirements. If any of the Optional Services are required by the Authority during the Term, the Authority will give notice to the Supplier in accordance with Clause 5.10 (Optional Services). The Authority is not obligated to take any of the Optional Services.

SCHEDULE 2 (Services Description)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

3.5.2 The Optional Services comprise:

- a) Mobile broadband airtime as stated in paragraph 3.2.6 of Annex A (WAN Technical Requirements) to Schedule 2 (Services Description);
- b) Not used;
- c) Not used;
- d) Data centre internet as stated in section 4.4.1 of Annex A (WAN Technical Requirements) to this Schedule;
- e) Not used;
- f) IPAM Service as stated in section 5.6.1 of Annex A (WAN Technical Requirements) to this Schedule; and
- g) SASE Services as stated in section 6 of Annex A (WAN Technical Requirements) and section 6.8.5 of Annex B (WAN Service Management Requirements) to this Schedule.

SCHEDULE 2 (Services Description)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

4.1 ANNEX A (WAN TECHNICAL REQUIREMENTS)

See:

Evolve - WAN Contract - Schedule 02 (Services Description) Annexes

4.2 ANNEX B (WAN SERVICE MANAGEMENT REQUIREMENTS)

See:

Evolve - WAN Contract - Schedule 02 (Services Description) Annexes

4.3 ANNEX C (WAN TRANSITION REQUIREMENTS)

See:

Evolve - WAN Contract - Schedule 02 (Services Description) Annexes

4.4 ANNEX D (WAN SOCIAL VALUE REQUIREMENTS)

See:

Evolve - WAN Contract - Schedule 02 (Services Description) Annexes

SCHEDULE 2 ANNEXES

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]



Ministry
of Justice

Schedule 2 (Services Description) Annexes

SCHEDULE 2 – ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX A – WAN TECHNICAL REQUIREMENTS

SCHEDULE 2 - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

1 Technical Requirements taxonomy

For information only, Figure 1 below provides a graphical view of the structure of these Technical Requirements.

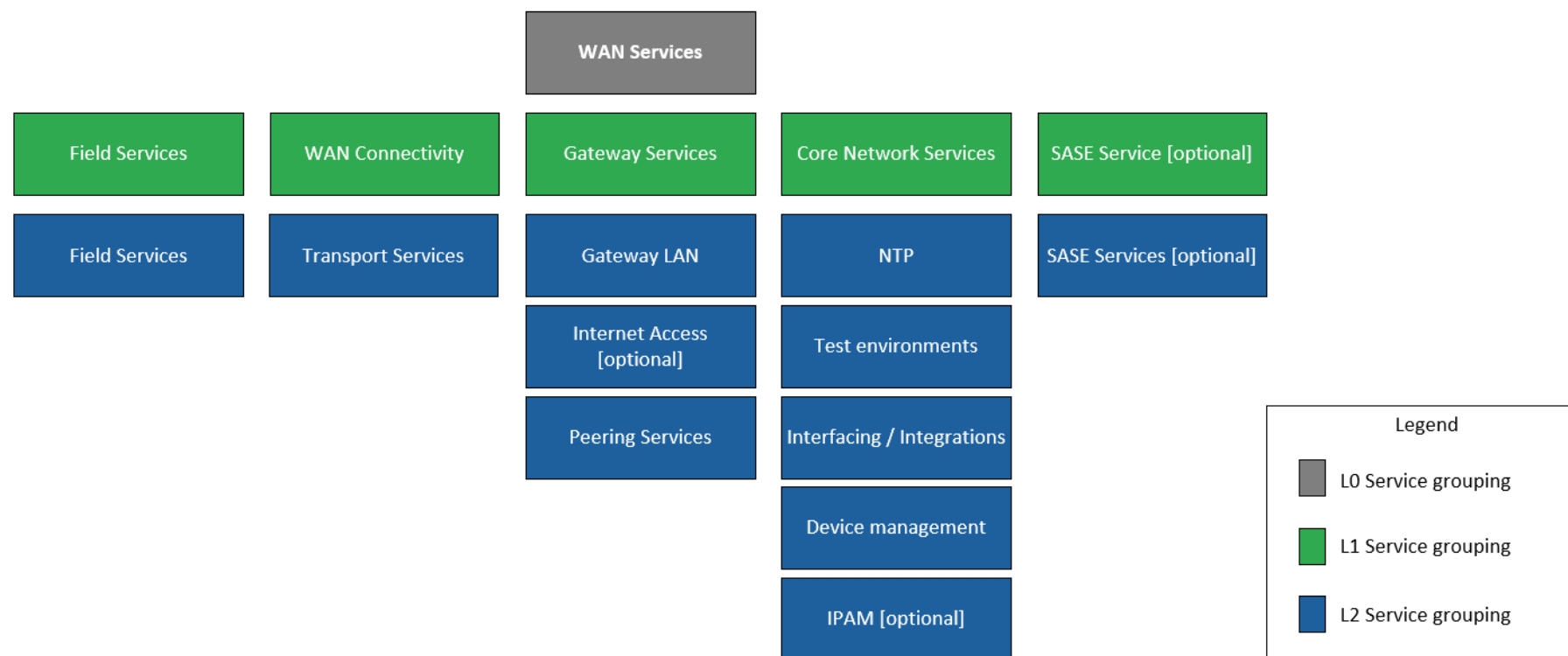


Figure 1: Technical requirements taxonomy

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Field Services

2.1 Service Taxonomy

For information only, Figure 2 below provides a graphical view of the structure of the Field Services requirements in this section 0.

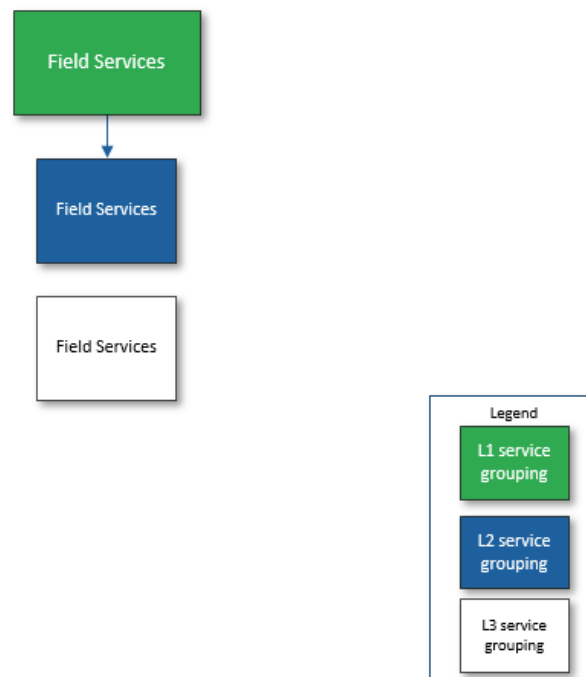


Figure 2 – Field Services Taxonomy

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

2.2 WAN Connectivity – Field Services

The Services described in this Paragraph 0 shall be conducted as required by the Authority under:

- a) the Implementation Plan; and/or
- b) any relevant Request.

2.2.1 Installation of Devices

2.2.1.1	The Supplier shall install Devices (including SD-WAN Edge Devices, any interface cards required for connection with upstream Devices, and intelligent power strips) at the Authority Sites in accordance with the WAN Cutover Approach.
2.2.1.2	Throughout and immediately following the Supplier's installation of SD-WAN Edge Devices, the Supplier's field engineers shall provide support from the Authority Site to coordinate with the Authority's network operations centre for: a) configuration of the Devices conducted remotely by the Authority; e.g. the Supplier shall apply IP configuration to enable the Device to establish connection with the internet and the Authority System; and b) testing of Devices conducted remotely by the Authority. Such Authority tests include connectivity, performance, failover and resilience testing.
2.2.1.3	The Supplier shall ensure that support provided by its field engineers under requirement 0 above is provided as described in the WAN Cutover Approach and includes support for bootstrap and zero-touch provisioning when required by the Authority.
2.2.1.4	Upon successful installation and deployment of Devices, including completion of Authority configuration and testing, the Supplier's field engineer shall confirm with the Authority's network operations centre that no further on-site support is required for the Device. Upon such confirmation, the Device will be considered to be within scope of the Authority System.
2.2.1.5	The Supplier shall comply with all building regulations and planning consents applicable when undertaking installation and cabling works at Authority Sites.
2.2.1.6	The Supplier shall in particular ensure that Field Services are delivered in accordance with the following Standards:

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

	a) MoJ ICT Physical Infrastructure Standards (including cabling colour coding standards); and b) Cyber and Technical Security Guidance.
2.2.1.7	The Supplier shall, unless otherwise requested, provide the cabling and patching between Devices where required to enable the delivery of the Services, including the necessary patch cables and patch leads, for connections between: a) the SD-WAN Edge Device(s) and the NTE; b) the SD-WAN Edge Device(s) and LAN Devices; and c) two SD-WAN Edge Devices. Where the Authority directs that such cabling and patching will instead be carried out by an Other Supplier, the Supplier shall liaise with such Other Supplier or with Authority in accordance with the Operational Interlock Document to coordinate cabling and patching with the Field Services.
2.2.1.8	The Supplier shall conduct Site readiness surveys, before any installation of Devices, to assess feasibility and readiness of an Authority Site for installing the Devices.
2.2.1.9	For installation of Devices at Authority Sites, the Supplier shall: a) follow the WAN Services Provisioning Process; b) plan and complete installation as described in the WAN Cutover Approach; c) request supply and delivery of the Devices from the Authority in accordance with the Device logistics arrangements agreed under Requirement 7.2.1.16 of the Transition Requirements; d) make a Record of proof of warranty (for example, whether the warranty label was intact on the Devices' packaging when delivered to the Supplier) or advise the Authority of any problems with doing so (e.g. the package being delivered without such label intact); e) verify that the correct Device(s) has/have been provided by the Authority; f) conduct all necessary hands-on aspects of installation, including racking, cabling, and power connection; and g) install SD-WAN Edge Devices within the same rack as the NTE unless otherwise agreed. If the Authority requires the SD-WAN Edge Device to be installed further from the NTE than can be accommodated by a 5 (five) metre cable run, the Supplier may take any impacts into consideration when submitting costed options under the WAN Services

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

	Provisioning Process described in Requirement 7.1.1.7 of the Transition Requirements and/or the Change Control Procedure.
2.2.1.10	The Supplier shall: a) confirm any requirements for the rack-mount kits within its site assessment, as conducted under technical requirement 0 above; and b) provide all necessary fittings for the rack-mount and for the cabling (e.g. cage nuts and bolts; any required cable management accessories). Note that the rack-mount kit will be provided by the Authority in accordance with the Authority Responsibilities.

2.2.2 Decommissioning of Devices

2.2.2.1	Subject to a relevant Request, the Supplier shall decommission Devices, including controlled disconnection from the Authority System, applying security controls to Authority Data as required, removal from rack and removal from the Authority Site.
2.2.2.2	Immediately prior to commencing decommissioning works of SD-WAN Edge Devices, the Supplier shall confirm with the Authority's network operations centre: a) the inventory and configuration details of the SD-WAN Edge Devices to be moved, including confirming model numbers, serial numbers, and current configuration; and b) that the Authority has taken a backup of the SD-WAN Edge Device data and remotely removed configurations from the Device.
2.2.2.3	Unless otherwise requested in writing by the Authority, the Supplier shall return the Devices to an Authority Site specified by the Authority at the time, always in compliance with the "MoJ Cyber and Technical Security Guidance" Standard, the Baseline Security Requirements and the Security Management Plan.
2.2.2.4	If requested by the Authority, the Supplier shall ensure that Authority Data is unrecoverable from the SD-WAN Edge Devices prior to removal of such Devices from Authority Sites, by use of destructive methods in compliance with the "MoJ Cyber and Technical Security Guidance" Standard.

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

2.2.3 Moves of Devices

2.2.3.1	Subject to a relevant Request, the Supplier shall relocate Devices from one Authority Site to another, including: a) controlled disconnection from the Authority System, working with the Authority's network operations centre as described in technical requirement 0 above; b) removal of the Device, the rack-mount kit from rack, and any associate cabling, including power cords; c) conveying the Devices and rack-mount kit to the destination Authority Site (always in compliance with the "MoJ Cyber and Technical Security Guidance" Standard, the Baseline Security Requirements and the Security Management Plan); and d) installation of the Device in accordance with Paragraph 0.

2.2.4 Field Services: general requirements

The following requirements apply to all the Field Services in this Paragraph 0.

2.2.4.1	The Supplier shall follow the Authority Site Access Request Process to: a) request access to Authority Sites; and b) request approval to proceed with the Field Services.
2.2.4.2	The Supplier shall update the Service Asset and Configuration Management System with the details of the relevant Device installed, moved or decommissioned.

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

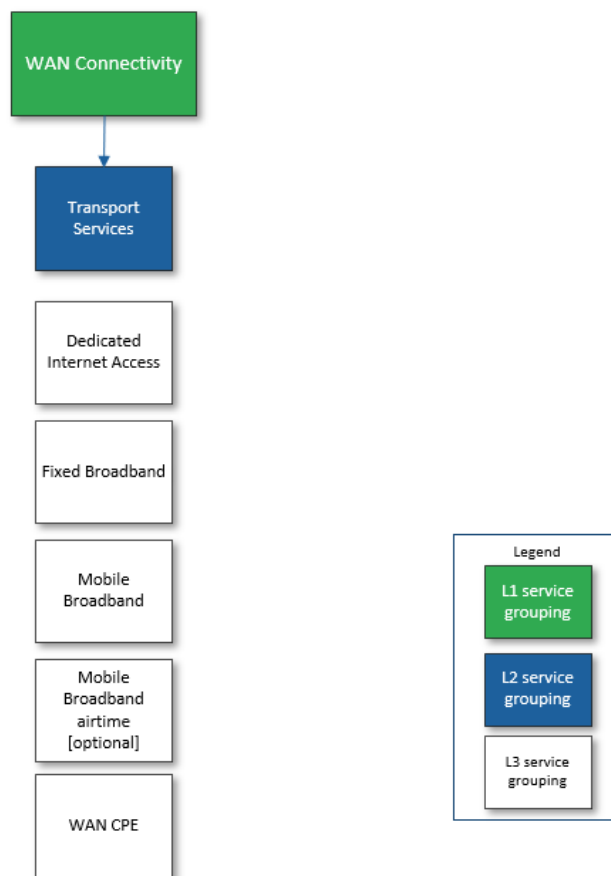
Security Classification (Official)

Contract reference: [REDACTED]

3 WAN Connectivity

3.1 Service Taxonomy

For information only, Figure 2 below provides a graphical view of the structure of the WAN Connectivity requirements in this section 3



SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

*Figure 3 – WAN Connectivity Services Taxonomy***3.2 WAN Connectivity – Transport Services****3.2.1 General**

3.2.1.1	The Supplier shall provide services that connect the Authority Sites to the internet, including all the requirements of this Paragraph 3.2 (“ Transport Services ”).
3.2.1.2	The Supplier shall be responsible for connecting the Access Circuits to the NTE and for connecting the NTE to the SD-WAN Edge Devices located at the Authority Sites and at such locations as directed by the Authority.
3.2.1.3	The Supplier shall be responsible for the provision of any cross site or long lined connections required for the connections stated in requirement 0 above.
3.2.1.4	The Supplier shall provide the WAN Connectivity as specified in the Authority Site Specification: a)for Authority Sites where “Dual link – internet transport” and “DIA” is specified, the Supplier shall provide dual and diverse DIA connectivity whereby, unless otherwise agreed in accordance with the WAN Services Provisioning Process, “dual” means two copper or two fibre connections using two NTE Devices (each connected to a separate SD-WAN Edge Device) and “diverse” means that each circuit is routed independently of the other, therefore with no single point of failure, between the NTE and each of the two separate points of presence; or b)for Authority Sites where “Single link – internet transport” and “DIA” is specified, the Supplier shall provide single-link DIA connectivity.
3.2.1.5	The Supplier shall be responsible for validating the redundancy, failover and full diversity of Transport Services at each Authority Site where delivered to ensure high availability and continuous connectivity in case of link failures. The validation report must be made available to the Authority and shall include: a)The testing criteria used to validate the high availability and full diversity; b)The results of the validation and testing; and

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

	c)The low-level site diagrams detailing the infrastructure including connection paths, Authority Comms Rooms, risers, ducts.
3.2.1.6	The Supplier shall provide Access Circuits to connect Authority Sites as specified in the Authority Site Specification.
3.2.1.7	The Supplier shall provide the committed data rate (CDR) that meet the throughput requirements for all Authority Sites as set out in the Authority Site Specification with the flexibility to increase or decrease the bandwidth as required.
3.2.1.8	The Supplier shall ensure the CDR provided at an Authority Site does not equal the Access Circuit capacity, unless otherwise agreed with the Authority.
3.2.1.9	The Supplier shall provide Transport Services that allows the Authority to procure additional bandwidth including based on: - a)The Authority Site bandwidth usage; - b)The Supplier's ongoing Authority Site bandwidth forecasts; - c)Technology and geographic constraints; and - d)The Authority's future business requirements. Such forecasts shall be based on a monthly Capacity Management review and ratified by the Authority.
3.2.1.10	The Supplier shall provide the most effective WAN connectivity to meet the requirements in the Authority Site Specification without constraint with regards to the provider of the underlying transport.
3.2.1.11	The Supplier shall manage all engagement with Access Circuit providers associated with installation and delivery of the WAN connectivity at Authority Sites.
3.2.1.12	The Supplier shall provide a Service that supports static IP address allocations to the Authority.
3.2.1.13	The Supplier shall provide the Authority with an integrated view of the Transport Service which includes: - a)Events relating to the circuits; - b)Network performance metrics; and - c)Current and historic circuit utilisation.

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

3.2.1.14	The Supplier shall be responsible for providing physical and logical connectivity from the WAN Service to the LAN Service and for ensuring that the WAN Service integrates seamlessly with the LAN Service.
3.2.1.15	The Supplier shall maintain a portfolio of broadband transport options, which reflect underlying changes and improvements in the marketplace including: a) Fixed broadband; b) Mobile broadband (as required); and c) Satellite broadband (as required).
3.2.1.16	The Supplier shall review and recommend enhancements to the broadband provisions, using the portfolio of broadband transport options supported in accordance with requirement 0, where substitution may provide enhancements in terms of capacity / price or speed of provisioning in accordance with Clause 8 (Services Improvement).
3.2.1.17	The Supplier shall be responsible for: a) All works, including all Civil Works and any Remediation outside the boundary of the Authority Sites that are required to deliver the Service; and b) Civil Works and Remediation inside the boundary of the Authority Sites where requested by the Authority through the Product and Service Catalogue.
3.2.1.18	The Supplier shall monitor the Services covering all relevant Performance Indicators in accordance with Schedule 3 (Performance Levels) and the performance metrics specified in technical requirement 0 below and implement any required tooling.
3.2.1.19	The Supplier shall provide data on the Performance Indicators in accordance with Schedule 3 (Performance Levels) and the performance metrics as specified in technical requirement 0 below as inputs into the Performance Monitoring Report.

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

3.2.1.20	The Supplier shall, as part of the acceptance into service of the Transport Services, test and validate the performance of the installed circuits including connectivity verification, latency, jitter and packet loss testing, at each Authority Site where delivered.
3.2.1.21	The Supplier shall conduct site readiness surveys, before any deployment of Transport Services, to assess feasibility and readiness of an Authority including to evaluate the physical locations where WAN circuits will be deployed, assessing distance, cabling and NTE placement.
3.2.1.22	The Supplier shall develop the high-level design describing the overall architecture, major components, their interactions and the description of the Services and Supplier Solution (“High Level Design”) and submit it to the Authority for review and Approval. Following the Authority’s Approval of the High Level Design, the Supplier shall produce detailed specifications and configurations of the individual components of the Services and Supplier Solution (“Low Level Designs”).
3.2.1.23	The Supplier shall be responsible for maintaining the High Level Design and Low Level Design documentation, ensuring the quality, accuracy and traceability of such documentation.
3.2.1.24	The Supplier shall submit the High Level Design, Low Level Design and related documentation for the Authority’s Approval. Formal Approval from the Authority is a prerequisite before commencing any build activities unless otherwise agreed with the Authority.
3.2.1.25	The Supplier shall provide suitably qualified and experienced technical resources to deliver the Technical Requirements as stated in this Annex A (WAN Technical Requirements).
3.2.1.26	Subject to any relevant Request, the Supplier shall conduct a desktop survey of potential Access Circuit locations (e.g. to support future planning).
3.2.1.27	Upon cease of any Access Circuit, the Supplier shall arrange and conduct removal and disposal of the relevant NTE and associated cabling.

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

3.2.1.28	Subject to any relevant Project Request, the Supplier shall decommission and securely dispose of WAN equipment of the Authority's former WAN suppliers at Authority Sites.

3.2.2 Not used

3.2.3 Dedicated Internet Access (DIA)

3.2.3.1	The Supplier shall provide internet connectivity services at Authority Sites as described within this Paragraph 0, as specified in the Authority Site Specification (and as required under Requests).
3.2.3.3	The Supplier shall ensure the internet connectivity services are provisioned to enable the following: a) Corporate usage – to include outbound web browsing for End Users, inbound remote access services for End Users wishing to connect to corporate services across the internet, and other corporate application services; b) Access to software as a service and other cloud services; and c) Third party services – to enable authorised and authenticated third party users, controlled access to specific systems for provision of support and maintenance services, and to enable automated outbound event, reporting or other data services required to deliver support services.
3.2.3.4	The Supplier shall provide default route information to the Authority for WAN Connectivity.
3.2.3.5	The Supplier shall provide and allocate sufficient RIPE addresses for use by the DIA service.
3.2.3.6	The Supplier shall provide the capability to deliver burstable bandwidth at Authority Sites, including where relevant under the Change and Evaluation Management Process and/or Change Control Procedure.
3.2.3.7	The Supplier shall provide the internet connectivity services which supports the following as a minimum: a) Border gateway protocol (BGP) for advanced routing and traffic management; b) Internet protocol suite; c) Applications such as VPNs, voice over IP and video conferencing; and

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

	d) Cloud-based services.
3.2.3.8	The Supplier shall provide internet connectivity services that meet the following network performance requirements unless otherwise agreed with the Authority in accordance with the Change Control Procedure: a) A maximum latency (average round trip-time) set by joint agreement of the Parties at the Service Review Board from time to time to reflect the Authority's business requirements and industry standards at the time, and in any case no more than 10 milliseconds when measured between the Authority Site and the Supplier's network edge (point of presence or internet edge router); b) A maximum latency (average round trip-time) of 10 milliseconds across the Supplier's UK IP core network; c) A packet loss rate of less than 0.1% during any 15 second interval; and d) A jitter of less than 15 milliseconds during any 15 second interval.

3.2.4 Fixed Broadband

3.2.4.1 A	The Supplier shall provide access to business grade fixed broadband as described in this Paragraph 3.2.4.
3.2.4.1 B	The Supplier shall ensure that broadband is provided with low contention and guaranteed support arrangements, and optimised to deliver cost-effective capacity, and satisfies a maximum contention ratio and a minimum download / upload requirement of 5:2 unless otherwise agreed with the Authority.
3.2.4.2	The Supplier shall provide fixed broadband services that supports a range of differentiated access technologies unless otherwise agreed with the Authority: a) Contended / uncontended; b) Symmetric / asymmetric; and c) Guaranteed / non-guaranteed.
3.2.4.3	The Supplier shall provide both Primary Fixed Broadband Services as well as a range of Ancillary Fixed Broadband Services through the Product and Service Catalogue:

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

	a)Primary Fixed Broadband Services provide fixed broadband connectivity as the primary WAN connection for an Authority Site with Performance Levels in accordance with Schedule 3 (Performance Levels); and b)Ancillary Fixed Broadband Services provide fixed broadband connectivity in addition to an Authority Site's primary WAN connectivity for specific use cases including support for card readers.
3.2.4.5	The Supplier shall provide fixed broadband services that provide and maintain resilient access to the internet which avoid single points of failure and meet the Target Performance Levels.
3.2.4.6	The Supplier shall provide fixed broadband services which support static IP addressing.
3.2.4.7	The Supplier shall ensure that all fixed broadband routers are installed with any Wi-Fi functionality disabled, unless otherwise requested by the Authority in writing.

3.2.5 Mobile Broadband

3.2.5.1 A	Subject to relevant Requests, the Supplier shall provide mobile broadband services as described within this Paragraph 3.2.5.
3.2.5.1 B	The Supplier shall ensure the mobile broadband services are capable of supporting 4G, 5G (or successor technologies where required) services and static IP addressing.
3.2.5.2	The Supplier shall provide, install, and configure mobile broadband devices capable of supporting 4G, 5G (or successor technologies where required) services in accordance with the Authority Site Specification.
3.2.5.3	Note that mobile broadband airtime is not in scope of this Paragraph 3.2.5.
3.2.5.4	The Supplier shall provide mobile broadband services with options for private access point name (APN) and soft SIM where supported by the SD-WAN Edge Devices.

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

3.2.6 Mobile Broadband Airtime (Optional Service)

Subject to implementation in accordance with the Optional Services Implementation Plan, the Supplier shall provide the Services described in this Paragraph 3.2.6.

3.2.6.1	The Supplier shall provide mobile broadband airtime services capable of supporting 4G, 5G (or successor technologies where required) services.
3.2.6.2	The Supplier shall provide SIM cards and mobile broadband plans to enable the provision of mobile broadband services.
3.2.6.3	The Supplier shall provide mobile broadband services with options for private access point name (APN) and soft SIMs where supported by the SD-WAN Edge Devices.

3.2.7 WAN CPE

3.2.7.1	The Supplier shall design, provide, install, configure, test, support (including onsite where necessary) and maintain the CPE necessary to deliver the Transport Service at each of the Authority Sites as stated in the Solution Design.
3.2.7.7	The Supplier shall ensure that CPE is resilient where required in accordance with the Authority Site Specification.
3.2.7.8	The Supplier shall ensure the CPE hardware is suitably sized to allow operation at the maximum Access Circuit capacity at the Authority Sites as stated in the Authority Site Specification, with all features and functionality enabled.

3.3 Not used

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

3.4 WAN Connectivity – Site Architectures

3.4.1 The Authority Sites in the Authority Site Specification shall each have one the following Site Architectures, as described in **Table 1** and Figure [4]:

- a) Data centre internet transport
- b) Split Site dual link – internet transport
- c) Dual link – internet transport
- d) Single link – internet transport
- e) Single link (broadband) – internet transport.

Table 1 - Site Architectures

Site Architecture	Transport	Hardware resilience
Data centre internet transport	High availability: - Dual Access Circuits providing assured internet transport - Active / active – failover using diversely routed Access Circuits	Dual SD-WAN Edge Devices (Resilient)
Split Site dual link – internet transport	High availability: - Single Access Circuit at each Authority Site (e.g. within a wider campus) providing assured internet transport - Active / active – failover between Authority Sites using point-to-point connections of the Authority System	Dual SD-WAN Edge Devices (Resilient)

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Dual link – internet transport	High availability: • Dual Access Circuits providing assured internet transport • Active / active – load balancing between the two links	Dual SD-WAN Edge Devices (Resilient)
Single link – internet transport	Single Access Circuit providing internet transport	Single SD-WAN Edge Device
Single link (broadband) – internet transport	Single fixed or mobile broadband link	Single broadband Device

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

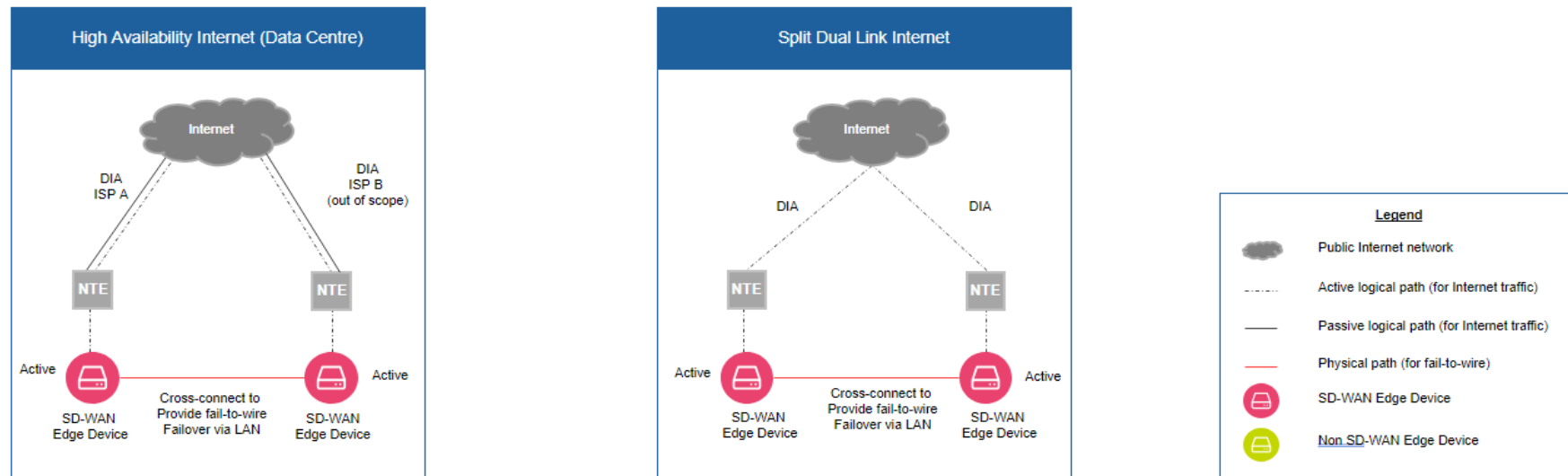
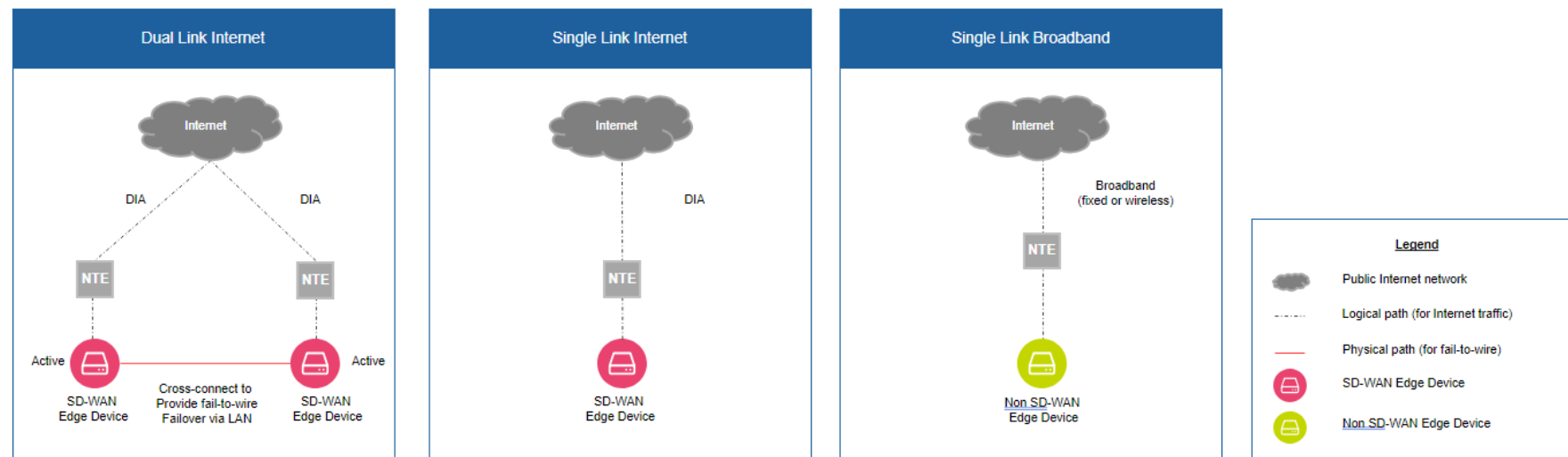


Figure 4 – Diagrams for WAN Site Architectures



SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

4 Gateway Services

4.1 Service Taxonomy

For information only, Figure 3 below provides a graphical view of the structure of the Gateway Services requirements in this section 4.

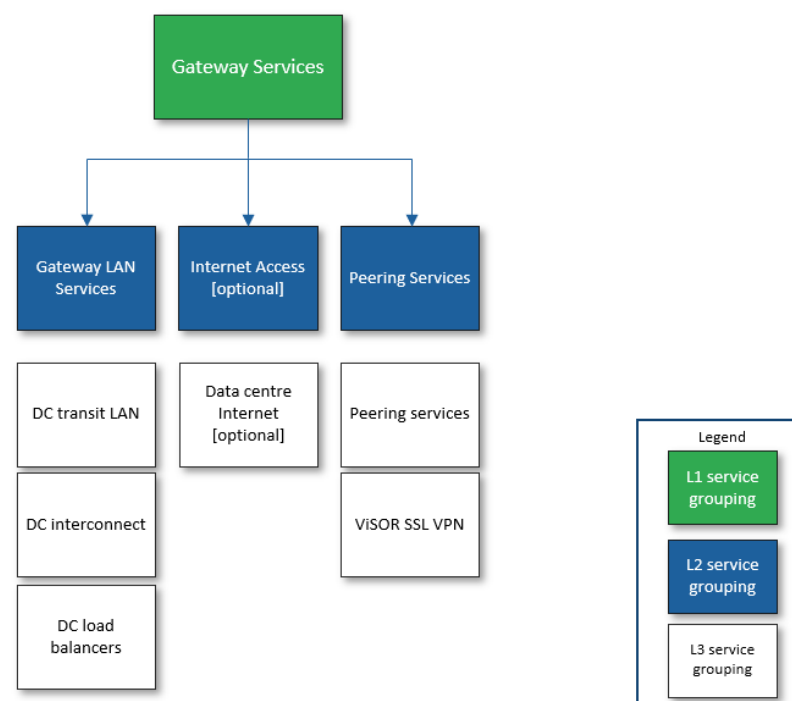


Figure 3 – Gateway Services Taxonomy

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

4.2 Gateway Services

4.2.1.1	The Supplier shall manage the Gateway System to provide integrated network services as described within this Paragraph 4 (the "Gateway Services").
4.2.1.2	The Supplier shall facilitate gateway services between various systems, including: a) protected and secure systems and the internet; b) Government secure systems; c) Authority/Service Recipient-controlled systems at different security levels; d) different OGDs' secure systems; e) secure systems of allied nations; f) remote access gateways; and g) Government and business services (e.g. electronic commerce, purchase to pay systems, human resources systems)
4.2.1.3	The Supplier shall manage and develop the Gateway System to deliver the Authority's desired outcomes, including to implement Changes and Service Changes required by the Authority. The Supplier shall be responsible for implementing the Authority's requirements (as may be updated from time to time under Requests for Change and/or the Change Control Procedure) in the Gateway System and the Supplier Solution. Key activities to be undertaken by the Supplier shall include: a) developing detailed design specifications based on the Authority's requirements; b) presenting design options for Authority review and approval; c) ensuring technical feasibility and adherence to Project scope; d) implementing the approved design in the Gateway System and/or Supplier Solution; e) impact assessment throughout the design process, including keeping the Authority informed design progress. f) validating/assuring any Authority-proposed changes to the Gateway System (including its design) and advise any impact to the IT Environment and/or Services;

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

	g) propose architectural design changes to the Authority based on Good Industry Practice; and h) producing, updating and maintaining the relevant High Level Design and Low Level Design.
4.2.1.4	The Supplier shall provide common security controls required for the delivery of services by Other Suppliers.
4.2.1.5	The Supplier shall provide the facility for the Other Suppliers to integrate, provide, maintain and support security controls specific to their services.
4.2.1.6	The Supplier shall integrate, provide, maintain and support security controls specific to the Services, in accordance with Schedule 4 (Standards) and Schedule 5 (Security Management).
4.2.1.7	The Supplier shall work and collaborate with the Other Suppliers who consume the Gateway Services. This collaboration shall ensure the effective provision of services by both the Supplier and the Other Suppliers.
4.2.1.8	The Supplier shall provide, manage and maintain Gateway Services between the Authority System and other IT environments to protect information assets at the same or different risk profiles, including the following types of environment: a) Authority System; b) Other Supplier IT environments; c) Public Services Network (PSN); and d) another external IT environments. The security controls to be implemented at Gateway shall be determined in accordance with Schedule 4 (Standards) and Schedule 5 (Security Management).
4.2.1.9	The Supplier shall monitor, manage, maintain and support the Gateway System in accordance with the Service Management Requirements.
4.2.1.10	The Supplier shall provide the Authority's network operations centre with read-only access to the Gateway System, facilitating the identification and diagnosis of network issues. This access shall allow the Authority to view routing information, device configurations, logs, and status information.

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

4.2.1.11	The Supplier shall utilise the Authority's designated identity source to authenticate End Users for read-only access to the Gateway System, unless otherwise agreed.
4.2.1.12	The Supplier shall provide the Authority's network operations centre with read-only access to the Supplier's monitoring data (including the live and historic data available to the Supplier) for the Gateway System.
4.2.1.13	The Supplier shall utilise the Authority's designated identity source to authenticate End Users for access to the Gateway System monitoring data, unless otherwise agreed.
4.2.1.14	The Supplier acknowledges and agrees to the Authority's refresh strategy for the Devices which form the Gateway System, being: a) in respect of Devices that are layer 2 switches which do not carry live user traffic only, to continue utilisation of the Device [REDACTED] until replacement is required owing to the Device failing; and b) in respect of all other Devices, to replace the Device prior to it becoming [REDACTED] unless there are reasons to continue utilisation of such Device (e.g. to support planned decommissioning of such Device), in which case such utilisation shall require risk assessment and impact assessment by the Parties and the period of such utilisation should be kept to a minimum.

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

4.3 Gateway Services – Gateway LAN**4.3.1 Gateway LAN Services**

4.3.1.1	The Supplier shall ensure that the Gateway System: - a)secures and facilitates the transfer of data between different network segments or Devices, enabling the flow of traffic between physical and logical networks including through and to the Authority Data Centres (“DC Transit LAN”); - b)enables seamless secure communication and data transfer between the Authority Data Centres (“DC Interconnect”); and - c)subject to a relevant Request, distributes incoming network traffic across multiple servers or resources locally and globally across the Authority’s network, ensuring optimal performance, high availability and scalability (“DC Load Balancers”).
4.3.1.2	When requested by the Authority, the Supplier shall make the services of the Gateway LAN available to Other Suppliers for the provision of services to the Authority utilising the Authority’s WAN (as provided by the Supplier under this Contract).
4.3.1.3	The Supplier shall manage and support the dark fibre or equivalent connectivity provided by Other Suppliers for the DC Interconnect cross-site connectivity between the Authority Data Centres.
4.3.1.4	Subject to a Request to include DC Load Balancers in scope of the Gateway Services, the Supplier shall: - a)manage and maintain the local and global load balancers’ integration with other systems; and - b)manage and maintain the capability for the Authority and relevant Other Suppliers to manage their respective data centre load balancer back-end pools.

4.3.2 Not used**4.3.3 Not used****4.3.4 Not used**

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

4.4 Gateway Services – Internet Access (Optional Service)**4.4.1 Data Centre Internet (Optional Service)**

Subject to implementation in accordance with the Optional Services Implementation Plan, the Supplier shall provide the Services described in this Paragraph 0.

4.4.1.1	The Supplier shall provide internet access at the Authority Data Centres as specified in the Authority Site Specification.
4.4.1.2	The Supplier shall provide resilient internet connectivity at the Authority Data Centres under a converged access model which allows the following as a minimum: - a)SD-WAN VPN termination; - b)third party VPN termination; - c)End User remote access termination; - d)outbound internet access; and - e)external-facing services.

4.5 Gateway Services – Peering Services**4.5.1 Peering services**

4.5.1.1	The Supplier shall provide, as a seamless service for the Authority and the Other Suppliers, integration of multiple separate networks and technical integration of the End to End Services, as described within this Paragraph 4.5.1 (the " Peering Services ").
4.5.1.2	The Supplier shall be a single point of responsibility for integrating multiple networks for the provision of services, including but not limited to:

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

	a) the physical and logical network design for the integration of multiple separate networks, as required by the Authority. This shall provide the seamless integration and transmission of traffic between the connected networks; b) the physical and logical network design for the separation of live environments and Non-Live Environments; and c) physical or logical separation of ICT Environments handling information assets at different risk profiles. d) efficient and resilient network routing of Authority data across the networks that are connected to the Network Interconnect Service; and e) management of IP Address conflicts and, where required, network address translation when integrating multiple networks.
4.5.1.3	The Supplier shall work and collaborate with the Authority and Other Suppliers to ensure that the functions of the Peering Services are fully available to the relevant services which use the Peering Services.
4.5.1.4	The Supplier shall utilise a resilient technical architecture for the Peering Services.
4.5.1.5	The Supplier shall manage and maintain the secure and resilient Network to Network Interconnect (NNI) gateway to enable connectivity between the Authority, Service Recipients, OGDs, the Supplier and Other Suppliers' or authorised third parties' services.
4.5.1.6	The Supplier shall provide a peering capability to support routing across networks of various risk profiles (including the any legacy network delivered under the Transitional Services) and between logical segments.
4.5.1.9	The Supplier shall establish the relationships and operational interfaces necessary to allow implementation and management of cross connect access to on-net transport partners, newly provisioned carrier services and partner organisations utilising the Authority Data Centres.

4.5.2 ViSOR (Violent & Sex Offenders Register) SSL VPN

4.5.2.1	The Supplier shall ensure the Gateway System provides remote access over the PSN to ViSOR for the End Users and/or Devices authorised by the Authority, including the SSL VPN termination.

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

4.5.2.2	The Supplier shall work with the EUCS Supplier to ensure the ongoing integration of the EUCS provided elements (EUCS firewall, devices that access the SSL VPN) with the Gateway System and Gateway Services and the effective end-to-end delivery of the access solution for the ViSOR application.

4.5.3 General

4.5.3.1	The Supplier shall collaborate with the Other Supplier(s) of data centre services for the Authority Data Centres as necessary to manage the Gateway System, including managing operational interfaces and relevant dependencies (e.g. access, power, cooling, cabling, engineering and support including “smart hands”, escorting).
4.5.3.3	Where the Supplier utilises Other Suppliers’ “smart hands” capabilities, the Supplier shall be responsible for specifying the required services and providing all appropriate instruction and agency management for the overall activity and delivery.

4.6 Not used

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

5 Core Network Services

5.1 Service Taxonomy

For information only, Figure 4 below provides a graphical view of the structure of the Core Network Services requirements in this section 5.

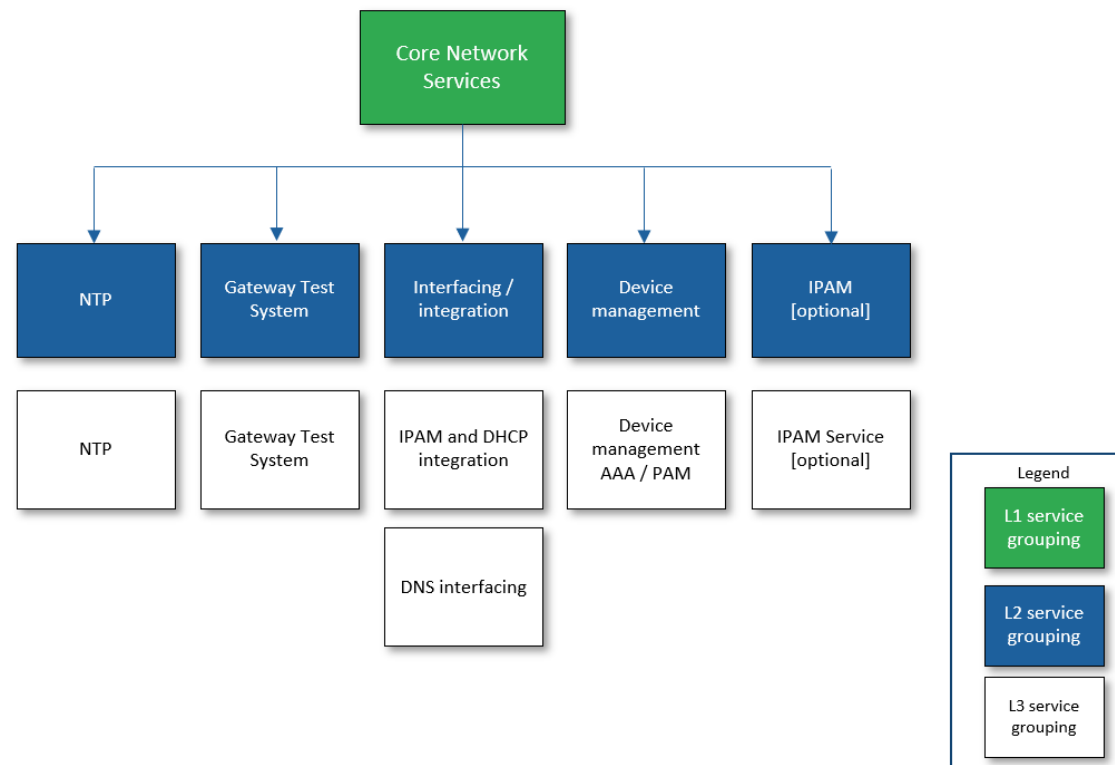


Figure 4 – Core Network Services Taxonomy

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

5.2 Core Network Services – NTP**5.2.1 NTP**

5.2.1.1 A	The Supplier shall provide access to a trusted time source to synchronise time across the components of the End to End Services, as described within this Paragraph 5.2 (“ Network Time Protocol ”).
5.2.1.1 B	The Supplier shall provide a highly available, secure, authenticated Master Time Reference (MTR) which shall be synchronised with an atomic NTP clock (or with a service that uses an atomic NTP clock to synchronise with) unless otherwise agreed with the Authority. The MTR stratum level shall be no less than stratum-2.
5.2.1.2	The Supplier shall ensure the MTR is available for use by the Authority, Service Recipients and Other Suppliers.
5.2.1.3	The Supplier shall interface with Other Suppliers to distribute the MTR as required.
5.2.1.4	The Supplier shall ensure that the MTR is synchronised with the NTP reference clock with a maximum offset of +/-10 milliseconds.
5.2.1.5	The Supplier shall monitor the MTR and NTP for availability, synchronisation accuracy, and compliance with Target Performance Levels. Additionally, the Supplier shall include the following in the Performance Monitoring Report: a) Uptime percentage of the MTR; and b) Minimum, maximum, and average time difference (offset) between the MTR and the reference source during the reporting period.
5.2.1.6	The Supplier shall maintain detailed Documentation of the NTP infrastructure and shall regularly review and update such Documentation to reflect any changes in the network.

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

5.3 Core Network Services – Gateway Test System**5.3.1 Gateway Test System**

5.3.1.1	The Supplier shall manage and develop the Gateway Test System in accordance with Paragraph 4.2.1.3 to provide and maintain a Non-Live Environment for testing (e.g. of the Authority's end user compute platform and devices).
5.3.1.2	The Supplier shall make the Gateway Test System available to Other Suppliers and/or the Authority's and Service Recipients' testers.
5.3.1.3	The Supplier shall, where required by the Authority, disconnect all relevant equipment operating in the Gateway Test System from the Master Time Reference service to enable testing to be performed.
5.3.1.4	The Supplier shall monitor, maintain and support the Gateway Test System in accordance with the Service Management Requirements.

5.4 Core Network Services – Interfacing / Integration**5.4.1 IPAM Integration**

5.4.1.1	The Supplier shall be responsible for managing the allocation of its IP addresses and subnets for the delivery of the Services interfacing with and utilising the Authority-provided IPAM toolset.
5.4.1.2	The Supplier shall efficiently assign IP prefix blocks to the Authority and Other Suppliers for their own allocation and management of these assigned address blocks through the Product and Service Catalogue.
5.4.1.3	The Supplier shall develop an IP Address Plan as part of the production of the Solution Design in accordance with the Detailed Implementation Plan. The IP Address Plan shall define how IP address blocks are distributed among authorised devices used in the delivery of ICT services to the Authority.
5.4.1.4	The Supplier shall manage the IP address allocation to Devices, as per the IP Address Plan as described in requirement 5.4.1.3 above for the Services.

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

5.4.1.5	The Supplier shall interface its IP address management tools and processes with the Authority's IP address management toolset or utilise the Authority's IP address management toolset directly.
5.4.1.6	The Supplier shall allocate valid IP addresses to the Authority and Other Suppliers upon request and maintain the list of available IP addresses in accordance with the IP Address Plan.
5.4.1.7	The Supplier shall deliver the same level of IP addressing support for both IPv4 and IPv6.

5.4.2 DNS Interfacing

5.4.2.1	The Supplier shall configure the IT Environment to forward all DNS requests to the Authority's DNS infrastructure.

5.5 Core Network Services – Device Management**5.5.1 Device Management AAA / PAM**

5.5.1.1	The Supplier shall provide a highly available and centralised privileged access management (PAM) service which performs authentication, authorisation and accounting (AAA) of access to Devices of the Gateway System, as described within this Paragraph 5.5 (" Device Management ").
5.5.1.3	The Supplier shall apply the "authenticate, authorise and accounting" (AAA) framework and enforce strong authentication (e.g. multi-factor authentication (MFA)).
5.5.1.4	The Supplier shall support a variety of authentication protocols including remote authentication dial-in user service (RADIUS) and TACACS+ for secure End User authentication.
5.5.1.5	The Supplier shall support multiple End User authentication methods, including: a) Username/password; b) Digital certificates; c) Token-based authentication; and

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

	d) Biometrics.
5.5.1.6	The Supplier shall provide Device Management using the Supplier System unless otherwise agreed in writing by the Authority.
5.5.1.7	Notwithstanding the Supplier's general obligations to manage PAM for the Supplier System (in accordance with Good Industry Practice and, where relevant, the Standards and Schedule 5 (<i>Security Management</i>)), Devices of the Supplier System are not in scope of Device Management under this Paragraph 5.5.

5.6 Core Network Services – IPAM (Optional Service)**5.6.1 IPAM Service (Optional Service)**

Subject to implementation in accordance with the Optional Services Implementation Plan, the Supplier shall provide the Services described in this Paragraph 5.6.1.

5.6.1.1	The Supplier shall provide IPAM in accordance with the Authority's IP addressing policy and as described within this Paragraph 5.6 (the "IPAM Service").
5.6.1.2	The Supplier shall ensure the IPAM Service is secure in accordance with the "MoJ Cyber and Technical Security Guidance" Standard and National Cyber Security Centre (NCSC) guidance.
5.6.1.3	The Supplier shall provide an IPAM toolset to manage and maintain the IP address schema and facilitate the allocation of IP addressing.
5.6.1.4	The Supplier shall manage the allocation of IP address ranges and subnets to the Authority and Other Suppliers where required.
5.6.1.5	The Supplier shall manage the Authority's IP address schema and make it available to the Authority and such Other Suppliers as the Authority shall require.
5.6.1.6	The Supplier shall provide the Authority and the relevant Other Suppliers with the ability to view, export and query the IP address management database.
5.6.1.7	The Supplier shall ensure the ranges of IP addresses used are scalable and efficiently reserved and allocated to accommodate future services as and when required by the Authority and/or the relevant Other Suppliers.

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

5.6.1.8	The Supplier shall work and collaborate with the Authority and the relevant Other Suppliers on the configuration of the dynamic IP address allocation service including address scopes and configuration to be applied to Devices.
5.6.1.9	The Supplier shall ensure the IPAM Service integrates with the Authority's DHCP service.

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

6 SASE Services (Optional Service)

Subject to implementation in accordance with the Optional Services Implementation Plan, the Supplier shall provide the Services described in this Paragraph 0 of this Annex A (WAN Technical Requirements).

6.1 The Authority may require the Services specified in Paragraphs 6.2 and 6.3 to support the SASE scope of the Authority System, being comprised of the following hardware and service subscriptions and/or functional equivalents or successors:

Vendor	Hardware, and service subscriptions	Category
[REDACTED]	[REDACTED] Hardware Appliance - Large Site	Hardware
[REDACTED]	[REDACTED] Premium Support	Support services subscription
[REDACTED]	[REDACTED] Hardware Appliance – Small Site	Hardware
[REDACTED]	[REDACTED] Premium Support	Support services subscription
[REDACTED]	SD-WAN [REDACTED] Subscription	Software subscription
[REDACTED]	SD-WAN [REDACTED] including [REDACTED]	Software subscription
[REDACTED]	[REDACTED]	Hardware
[REDACTED]	[REDACTED]	Support services subscription

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

[illegible]

SCHEDULE 2 (Services Description) - ANNEX A (WAN TECHNICAL REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

[illegible]

6.2 Where required in accordance with Clauses 5.10, 5.11 and 5.12, the Supplier shall act as a reseller to the Authority of service subscriptions from the vendor(s) of the SASE scope of the Authority System.

6.3 Subject to a relevant Request, the Supplier shall provide professional services for SASE and SD-WAN (e.g. design, architecture, testing, project activity, security services, network optimisation).

SCHEDULE 2 - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX B – SERVICE MANAGEMENT REQUIREMENTS

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

These requirements comprise:

- the standard Service Management Requirements, which support the Authority's standard service operations' approach to managing technology services (paragraphs 6.1 to 6.7); and
- the WAN Service Management Requirements, which are specific to this Contract;

together, the "**Service Management Requirements**".

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

6.1 – 6.7 Standard Service Management Requirements

The following requirements support the Authority's service operations' standard approach to managing services across its suppliers and in-house services.

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.1.1.2.	General Principles	General	The Supplier shall, at all times, protect the confidentiality, integrity and availability of the Services, Authority System and Authority Data.
6.1.1.3.	General Principles	General	The Supplier shall, with regards to Service Management; design, transition, operate and continually improve the Services in accordance with the Processes.
6.1.1.7.	General Principles	General	The Supplier shall provide support to the Authority, as reasonably required, in order to maintain the Authority's Service Management policies, processes and procedures.
6.1.1.8.	General Principles	General	The Supplier shall adopt any changes made to the Authority's Service Management policies, processes and procedures throughout the Term that are agreed through the governance framework set out in Schedule 21 (Governance).
6.1.1.13.	General Principles	General	The Supplier shall follow the Demand Management Process
6.1.1.14.	General Principles	General	The Supplier shall, where applicable, adopt the Authority's naming standards and conventions.
6.1.8.1.	Service Strategy	Demand Management	The Supplier shall provide progress notifications to the Authority in relation to any open Demand Requests including:

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
			1. Commercial sign-off completion; 2. Solution manager allocation; and 3. Implementation completion.
6.1.8.2.	Service Strategy	Demand Management	The Supplier shall provide reporting on the status of Demand Requests for each Service Period.
6.1.8.3.	Service Strategy	Demand Management	The Supplier shall ensure that where Demand Management information is recorded that the Authority's Demand Management System is used to record it and thus either: a)utilise the Authority's Demand Management System; or b)operate its own Demand Management system ensuring that it integrates in near real time with the Authority's Demand Management System.
6.2.1.1.	Service Strategy	Demand Management	The Supplier shall provide relevant financial information to the Authority where requested either via the Project Initiation Process or Change Control Procedure or Change and Evaluation Management Process in order to input into detailed business cases for proposed new or changed services.
6.2.1.2.	Service Strategy	Demand Management	The Supplier shall respond to Demand Requests from the Authority in accordance with the Project Initiation Process (as defined in Schedule 22 (<i>Change Control Procedure</i>)).
6.2.1.4.	Service Strategy	Service Portfolio Management	The Supplier shall ensure the Service Portfolio for the Services is accurate and correct and continually updated.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.2.1.5.	Service Strategy	Service Portfolio Management	The Supplier shall (subject to the Document Approval Procedure) create and update Service Design Packages for the Services and manage these in line with the Service Management requirements 6.4.2.6 to 6.4.3.1 (Knowledge Management).
6.2.2.1.	Service Strategy	Service Portfolio Management	The Supplier shall, upon commissioning of a new service, provide the Service Design Package to the Authority within one (1) Month of commissioning the service.
6.2.3.1	Service Strategy	Service Portfolio Management	The Supplier shall ensure that the information it provides with regards to the Service Portfolio sets out: 1. A complete description set of the Services provided by the Supplier to the Authority; 2. The service pipeline for any service in development (including planned changes to the Services, the introduction of any new service and technical refresh of the existing Services); and 3. Any service currently being retired or in the process of being decommissioned.
6.2.3.2	Service Strategy	Service Portfolio Management	The Supplier shall ensure that where Service Portfolio Management information is recorded that the Authority's Service Portfolio Management System is used to record it and thus either: a) utilise the Authority's Service Portfolio Management System; or b) operate its own Service Portfolio Management system ensuring that it integrates in near real time with the Authority's Service Portfolio Management System.
6.2.3.3	Service Design	Risk Management	The Supplier shall conduct proactive monitoring to identify any emergent risk to the provision of the Services and End to End Services. The Supplier shall report these

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
			emergent risks immediately to the relevant risk review board in accordance with Schedule 21 (<i>Governance</i>).
6.2.3.4	Service Design	Risk Management	The Supplier shall, in accordance with Schedule 21 (Governance) attend risk review boards, develop and manage risk action plans, and recommend to the Authority appropriate measures to mitigate any risks identified.
6.2.3.5	Service Design	Risk Management	The Supplier shall only implement risk mitigation measures approved by the Authority in accordance with the relevant Process.
6.3.1.1	Service Design	Availability Management	The Supplier shall make available to the Authority information which relates to the availability of Operational Services, in near real time.
6.3.1.3	Service Design	Availability Management	The Supplier shall produce a service component failure impact analysis that identifies the impact of a component failure. The Supplier will produce this prior to the relevant Services being accepted into service.
6.3.1.4	Service Design	Availability Management	Where component failure has led to an Incident, analysis of the failure will form part of the Root Cause Analysis for any Incidents, and produced within the timeframe defined by the Incident Management Process.
6.3.1.5	Service Design	Availability Management	The Supplier shall work with the Authority to test the end to end availability reporting mechanism and integration with the ITSM Toolset.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.3.1.6	Service Design	Availability Management	The Supplier shall operate its own availability management system ensuring that it integrates in near real time with the Availability Management System.
6.3.2.1	Service Design	Capacity Management	The Supplier shall operate effective processes to ensure that the capacity of the Services and the supporting resources are delivered in accordance with the Performance Indicators in Schedule 3 (Performance Levels) and shall manage the capacity of the Services in a cost-effective and timely manner and in accordance with the Capacity Management Policies and the Processes (" Capacity Management Services ").
6.3.2.2	Service Design	Capacity Management	The Supplier shall provide tooling for the purposes of managing, monitoring and reporting on the capacity of the Services.
6.3.2.3a	Service Design	Capacity Management	The Supplier shall provide the Authority with access to the Supplier's capacity management tooling either through integration with the ITSM Toolset or by providing the Authority with direct access to the Supplier's tooling.
6.3.2.3b	Service Design	Capacity Management	The Supplier shall pro-actively monitor the Services for capacity related Events and respond to any capacity-related Events to ensure that the Target Performance Levels are met.
6.3.2.4	Service Design	Capacity Management	The Supplier will notify the Authority of any warning or exception type capacity Events by raising these with the Authority in near real time.
6.3.2.5	Service Design	Capacity Management	The Supplier shall deliver a report on a monthly basis at the Service Review Board that includes, as a minimum:

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
			a) a detailed view of bandwidth utilisation against each Authority Site; b) a detailed view of where utilisation is above or below the normal range against each Authority Site; c) recommendations to ensure that capacity is managed across the Services and the Gateway System in the most cost-effective manner; d) a summary view of expected future demand based on analysis of Demand Requests, Service Changes, Change Requests and Service Requests raised including analysis to show impact on capacity and recommendations to address additional demand; e) recommendations for specific mitigating actions to manage utilisation across the Services and the Gateway System. f) a risk management plan and capacity forecast; and, g) analysis of actual performance in the Service Period against the previous month's capacity forecast; (the " Capacity Report ").
6.3.2.6	Service Design	Capacity Management	The Supplier shall produce and maintain a capacity plan on an annual basis that will include as a minimum: a) Trending of utilisation across all Authority Sites for the period; b) Bandwidth optimisation – recommendations on how to optimise bandwidth utilisation; c) Traffic analysis; d) Scalability and redundancy – how will the Supplier scale to meet demand or deal with redundancy; e) Risk assessment – risks and mitigating strategies; and f) Recommendations to manage future demand – strategic view including recommendations around technology;

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
			g) an executive summary; (the “ Capacity Plan ”). The Supplier shall provide the Capacity Plan each year and shall provide updates each Quarter to the Capacity Plan and shall present the Capacity Plan (as updated) at the Service Review Board.
6.3.2.7	Service Design	Capacity Management	The Supplier will identify and propose Catalogue Items for inclusion in the Product and Service Catalogue to deliver capacity changes in line with the Demand.
6.3.2.8	Service Design	Capacity Management	The Supplier shall manage the availability of IT resources and IT Personnel to meet the forecasted demands to support the Services.
6.3.3.1	Service Design	IT Service Continuity Management	The Supplier shall support and complete all agreed actions in relation to the ITSCM planning process ensuring its ITSCM Plan aligns to the Authority's ITSCM requirements.
6.3.3.2	Service Design	IT Service Continuity Management	The Supplier shall work collaboratively with the Authority and Other Suppliers to ensure that its ITSCM Plan aligns with those of Other Suppliers engaged in the provision of the End to End Services to the Authority.
6.3.3.3	Service Design	IT Service Continuity Management	The Supplier shall develop, maintain and provide an up-to-date ITSCM Plan, which is tested at least annually. The Supplier shall update the ITSCM plan following live/test invocations and / or significant changes to the functionality of the Services.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.3.4.1	Service Design	IT Service Continuity Management	The Supplier shall: a) clearly and unambiguously define triggers for ITSCM invocation and closure points within the ITSCM plans; and b) review and agree those triggers and closure points with the Authority as part of approval of ITSCM Plan in accordance with Schedule 26 (Service Continuity Plan and Corporate Resolution Planning).
6.3.4.2	Service Design	IT Service Continuity Management	The Supplier shall ensure that any business impact analyses or risk assessments undertaken by the Authority and presented to the Supplier are factored into its ITSCM Plan(s) for the Services.
6.3.4.3	Service Design	IT Service Continuity Management	The Supplier shall provide the Authority with a SPoC (Single Point of Contact) for the ITSCM Plan and provide an escalation process with full contact details.
6.3.4.4	Service Design	IT Service Continuity Management	The Supplier shall ensure that the Supplier's SPoC (or a designated substitute if the SPoC is unable to attend) is available to attend the Risk Management Board or such other meetings as may be agreed from time to time in accordance with Schedule 21 (<i>Governance</i>). The Supplier's SPoC shall record and complete all of the Supplier's agreed actions deriving from each such meeting.
6.3.4.5	Service Design	IT Service Continuity Management	Within three (3) months of the Effective Date, the Supplier shall provide Authority-approved ITSCM awareness and training for all Supplier Personnel with ITSCM-related duties.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.3.4.6	Service Design	IT Service Continuity Management	The Supplier shall ensure that all relevant Supplier Personnel maintain full awareness of the stages within the Supplier's ITSCM Plan and be able to evidence this on request, through training records or equivalent.
6.3.4.7	Service Design	IT Service Continuity Management	The Supplier shall notify the Authority of the occurrence of any ITSCM Event and shall provide formal recommendations for invoking the relevant ITSC Plan(s) to ensure that Services are delivered with the agreed recovery objectives.
6.3.4.8	Service Design	IT Service Continuity Management	The Supplier shall be required to invoke immediately any ITSC Plan when requested to do so by the Authority.
6.3.4.9	Service Design	IT Service Continuity Management	The Supplier shall issue a post-test report to the Authority within 20 Working Days of each ITSC Plan test, together with remediation plans including a possible retest to resolve failed tests.
6.3.4.10	Service Design	IT Service Continuity Management	The Supplier shall proactively monitor the Services, identifying risks and proposing actions to mitigate those risks and capture the output in the ITSC Plan.
6.3.4.11	Service Design	IT Service Continuity Management	The Supplier shall support the Authority and Other Suppliers in the planning, implementation, execution and closure of IT Service Continuity Management testing for End to End Services, on at least an annual basis.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.3.4.12	Service Design	IT Service Continuity Management	The Supplier shall participate in the Authority's IT Service Continuity Management test exercise regime and undertake the relevant activities in compliance with the Authority's ITSCM Test Schedule.
6.3.4.13	Service Design	IT Service Continuity Management	The Supplier shall ensure that IT Service Continuity Management is consistent with ISO27031 and to the standards specified in the relevant ITSCM Plan.
6.3.4.14	Service Design	IT Service Continuity Management	Prior to any Operational Service Commencement Date, the Supplier shall prepare and deliver, for the Authority's written approval a plan which shall detail the process and arrangements that the Supplier shall follow to ensure continuity of the Services.
6.3.4.15	Service Design	IT Service Continuity Management	Following the closure of any ITSCM event, the Supplier shall provide the Authority with information, guidance and assistance as reasonably required to support the Major Incident Management Process, including to support the production of the Authority's Major Incident report.
6.3.4.16	Service Design	Service Catalogue Management	The Supplier shall follow the Product and Service Catalogue Management Process and use the Product and Service Catalogue to make Catalogue Items available. In order for a Catalogue Item to be considered for inclusion in the Product and Service Catalogue, the item must comply with the Standards and, in addition to the requirements of Paragraph 3 of Part B to Annex 2 of Schedule 22 (<i>Change Control Procedure</i>), as a minimum: a) Have a clear description; b) Be fixed price or nil charge; c) Have a defined fulfilment flow; and

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
			d)Have a defined lead time to fulfil the Service Request.
6.3.4.17	Service Design	Service Catalogue Management	The Supplier shall ensure that all Catalogue Items have appropriate Service Assets and Configuration Items identified within the Service Asset and Configuration Management System where applicable.
6.3.4.18	Service Design	Service Catalogue Management	The Supplier shall utilise the Product and Service Catalogue Management system / ITSM Toolset to manage and maintain all Catalogue Items. The Supplier shall be responsible for checking and identifying errors and omissions in the Product and Service Catalogue and shall promptly report any such errors or omissions to the Authority and apply corrections as necessary.
6.3.5.1	Service Design	Service Catalogue Management	The Supplier shall regularly review all Demand Requests and Project Requests and identify potential candidates for inclusion in the Product and Service Catalogue as Catalogue Items, for consideration by the Authority. If approved by the Authority, the Supplier shall make such Catalogue Items available on the Product and Service Catalogue.
6.3.5.2	Service Design	Service Catalogue Management	The Supplier shall work with the Authority to identify new Catalogue Items and regularly review and optimise existing Catalogue Items in the Product and Service Catalogue.
6.3.5.3	Service Design	Service Level Management	The Supplier shall provide a dedicated Service Manager, who shall be Key Personnel responsible for interfacing with the Authority's Service Level Management function and for ensuring the Services are managed to meet the Target Performance Levels.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.3.5.4	Service Design	Service Level Management	The Supplier shall ensure that where Service Level Management information is recorded that the Authority's Service Level Management System is used to record it and thus either: a)utilise the Authority's Service Level Management System; or b)operate its own Service Level Management system ensuring that it integrates in near real time with the Authority's Service Level Management System.
6.3.5.5	Service Design	Supplier Management	Working with the Authority, the Supplier shall, in accordance with Paragraph 1.2 of Part B of Schedule 3 (<i>Performance Levels</i>), establish a Performance Monitoring Report and Balanced Scorecard Report for the Services.
6.3.6.3	Service Design	Supplier Management	The Supplier shall provide all management and performance information required by the Authority in support of the production of a regular Performance Monitoring Report and Balanced Scorecard Report.
6.3.6.5	Service Design	Supplier Management	The Supplier shall identify, report and manage risks to the Services supply chain in order to support the delivery of performance against any Performance Indicators.
6.3.7.3	Service Design	Supplier Management	The Supplier shall provide copies of all contractual material in a way that is accessible by the Authority using its systems.
6.3.7.4	Service Transition	Transition Planning and Support	Where agreed via the Change Control Procedure or the Change and Evaluation Management Process, the Supplier shall support the Authority in the discovery, identification, and agreement of any service requirements necessary to transition a service.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.3.7.5	Service Transition	Transition Planning and Support	Where agreed via the Change Control Procedure or the Change and Evaluation Management Process, the Supplier shall provide or input into the design of new or changed Services.
6.3.7.7	Service Transition	Transition Planning and Support	Where agreed via the Change Control Procedure or the Change and Evaluation Management Process, the Supplier shall develop a transition plan with the Authority that covers the scope of the of the content of the change or Request.
6.4.1.1	Service Transition	Transition Planning and Support	Where a transition plan is agreed via the Change Control Procedure or in a Project Request or via Change and Evaluation Management Process or as part of a Request, the Supplier shall support the Authority in ensuring that sufficient and appropriate resources are identified and available to deliver the relevant transition plan to time, quality and cost constraints.
6.4.1.2	Service Transition	Transition Planning and Support	Prior to implementing Services which will impact the Authority's live services, the Supplier shall gain Approval for the relevant Services' Service Design Package(s).
6.4.1.3	Service Transition	Transition Planning and Support	Where agreed via the Change Control Procedure or the Change and Evaluation Management Process or in a Project Request, the Supplier shall be responsible for the creation of an early life support plan for a new service or change to a service.
6.4.1.4	Service Transition	Transition Planning and Support	The Supplier shall ensure that during the course of implementing or amending Services, the integrity of in situ deliverables, service components and Configuration Items is maintained.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.4.1.6	Service Transition	Transition Planning and Support	The Supplier shall ensure that where transition planning and support information is recorded that the Transition Planning and Support System is used to record it and thus either: a)utilise the Transition Planning and Support System where possible; or b)operate its own transition planning and support system ensuring that it integrates with the Transition Planning and Support System.
6.4.1.7	Service Transition	Transition Planning and Support	The Supplier shall identify and document any service dependencies or changes to service dependencies resulting from Requests, Service Changes, Operational Changes or the Change Control Procedure, and submit these to the Authority.
6.4.1.9	Service Transition	Change and Evaluation Management	The Supplier shall follow the Change and Evaluation Management Process and ensure that all RFCs submitted contain the appropriate level of detail as required by the Authority.
6.4.1.10	Service Transition	Change and Evaluation Management	The Supplier shall participate in the activities of the 'Change Advisory Board' (CAB) (which shall occur not less than once a month) and the Emergency CAB (ECAB) (which shall convene as required), to review changes including: a)Reviews Request for Change (RFCs); b)Approval of Changes; and c)Retrospective change approvals, as further described in the CAB terms of reference and the E-CAB terms of reference, ("Change Advisory Board" or "CAB" and Emergency CAB or ECAB).

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.4.2.1	Service Transition	Change and Evaluation Management	The Supplier shall provide all information relating to Service Changes to the Authority for inclusion in the ITSM Toolset.
6.4.2.2	Service Transition	Change and Evaluation Management	The Supplier shall inform the Authority of any backed out or Failed Changes as set out in the Change and Evaluation Management Process.
6.4.2.3	Service Transition	Change and Evaluation Management	The Supplier shall perform an Impact Assessment against the introduction of any new or changed Service as part of the Change and Evaluation Management Process.
6.4.2.4	Service Transition	Change and Evaluation Management	The Supplier shall participate and contribute to post implementation reviews.
6.4.2.5	Service Transition	Change and Evaluation Management	The Supplier shall ensure that change management information is recorded within the Change Management System. The Supplier may either: a) utilise the Change Management System; or b) operate its own change management system ensuring that such system integrates in near real time with the Change Management System.
6.4.2.6	Service Transition	Knowledge Management	The Supplier shall be responsible for the production, maintenance and assurance of up-to-date information for inclusion in the Authority's Knowledge Management System(s), to include:

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
			1. Methods to resolve Incidents; 2. Known errors; 3. Minimum data set information; 4. Frequently asked questions; 5. Self-help articles; and 6. Any other knowledge or data relevant to the running of the Operational Service.
6.4.2.7	Service Transition	Knowledge Management	When knowledge data relating to the Services in the Knowledge Management System is found to be inaccurate, incomplete or lacks integrity, the Supplier shall be responsible for making the Authority aware and then, upon agreement, correcting or removing such data.
6.4.2.8	Service Transition	Knowledge Management	Where required, the Supplier shall ensure Supplier Personnel complete any required training in the use of the Knowledge Management System.
6.4.3.1	Service Transition	Knowledge Management	The Supplier shall utilise the Knowledge Management System.
6.4.3.2	Service Transition	Release and Deployment Management	The Supplier shall provide release plan(s) covering a two (2) month rolling period to the Authority.
6.4.3.3	Service Transition	Release and Deployment Management	The Supplier shall provide documentation to the Authority, including: 1. Release plans; 2. Release packages; and 3. Implementation activities.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.4.3.4	Service Transition	Release and Deployment Management	The Supplier shall support the Authority in maintaining and updating the release schedule.
6.4.4.1	Service Transition	Release and Deployment Management	The Supplier shall work and collaborate with the Authority to plan and implement release activity to ensure that any business disruption is minimised.
6.4.4.2	Service Transition	Release and Deployment Management	The Supplier shall ensure that where Release and Deployment Management information is recorded that the Release and Deployment Management System is used to record it and thus either: a)utilise the Release and Deployment Management System; or b)operate its own release and deployment management system ensuring that it integrates in near real time with the Release and Deployment Management System.
6.4.4.3	Service Transition	Service Asset and Configuration Management	The Supplier shall ensure that Configuration Items relating to the Services are identified and their relationships recorded and reported to the Authority.
6.4.4.4	Service Transition	Service Asset and Configuration Management	The Supplier shall maintain accurate records of all Configuration Items and Service Assets used to deliver the Services. This includes both Supplier-owned and Authority-owned Configuration Items and Assets.
6.4.4.5	Service Transition	Service Asset and Configuration Management	Not Used

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.4.5.1	Service Transition	Service Asset and Configuration Management	The Supplier shall ensure that where Service Asset and Configuration Management information is recorded that the Service Asset and Configuration Management System is used to record it and thus either: a)utilise the Service Asset and Configuration Management System; or b)operate its own Service Asset and Configuration Management system ensuring that it integrates in near real time with the Service Asset and Configuration Management System.
6.4.5.2	Service Transition	Service Asset and Configuration Management	Not Used.
6.4.5.3	Service Transition	Service Asset and Configuration Management	The Supplier shall securely remove and dispose of Assets and Authority Assets where such assets are identified as redundant and shall securely dispose of removable media.
6.4.5.4	Service Transition	Service Asset and Configuration Management	The Supplier shall, at minimum, comply with the Authority's minimum data set (schema) for Service Asset and Configuration Management.
6.4.5.5	Service Transition	Licence Management and Compliance	The Supplier shall be responsible for the provision and renewal of all Software licences and certificates in accordance with Clause 3.2(j) (Warranties).

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.4.5.6	Service Transition	Licence Management and Compliance	The Supplier shall capture, manage and monitor Software licence usage and ensure that such usage is legal and provide this information each Service Period to the Authority. As a minimum, the information shall include the: a)Product; b)Edition; c)Version details of the software licences consumed and utilisation; d)Licence entitlement details including term; and e)Hardware information relevant to licence consumption, such as processor type and/or power, number of cores, and virtualisation configuration details.
6.4.5.7	Service Transition	Licence Management and Compliance	The Supplier shall be responsible for the ongoing management and monitoring of Software licence usage in order to ensure that such usage is both legal, compliant and efficient, including the enablement of licence redeployment to minimise licence costs.
6.4.6.1	Service Transition	Licence Management and Compliance	The Supplier shall ensure that Software deployed as part of the Services is efficiently, effectively and when possible, automatically removed or redeployed across the IT Environment as required.
6.4.6.2	Service Transition	Licence Management and Compliance	The Supplier shall allow the Authority to request the installation and configuration of tools for the purpose of monitoring the presence of unauthorised or unlicensed Software.
6.4.6.3	Service Transition	Licence Management and Compliance	The Supplier shall ensure that where licence management information is recorded that the Licence Management System is used to record it and thus either: a)utilise the Licence Management System; or

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
			b)operate its own licence management system ensuring that it integrates in near real time with the Licence Management System.
6.4.6.4	Service Transition	Licence Management and Compliance	Not Used.
6.4.6.5	Service Transition	Service Validation and Testing	The Supplier shall be responsible for the planning, design, implementation, execution and reporting of: 1. System integration testing. 2. Operational acceptance testing. 3. Service acceptance testing; 4. Unit/component testing; 5. System testing; and 6. Information security testing.
6.4.6.6	Service Transition	Service Validation and Testing	The Supplier shall support the Authority in the planning, design, implementation, execution and reporting of: 1. User acceptance Testing; 2. Service management acceptance Testing; and 3. Pilot Testing.
6.4.6.7	Service Transition	Service Validation and Testing	The Supplier shall identify an appropriately qualified Test Manager who shall be fully accountable for all Service Validation and Testing performed and/or supported by the Supplier during the Term.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Require ment #	Level 2 Category	Level 3 Category	Requirement
6.4.7.2	Service Transition	Service Validation and Testing	The Supplier shall, when required by the Authority as part of a Request, Service Change or Project Work Order, produce a programme/project Test Strategy and/or project/release Test Plan and submit to the Authority for approval, in accordance with Schedule 14 (<i>Testing Procedures</i>).
6.4.7.4	Service Transition	Service Validation and Testing	The Supplier shall be responsible for the provision of an up-to-date record of all Test results, including supporting evidence for any Test that the Supplier is responsible for, irrespective of whether the Tests were successful or unsuccessful.
6.4.7.5	Service Transition	Service Validation and Testing	The Supplier shall provide, maintain and support Test management tool(s) for the purposes of delivering the Services.
6.4.7.6	Service Transition	Service Validation and Testing	The Supplier shall ensure that all test deliverables and Configuration Items it has created or modified, are managed to the required standard
6.4.7.7	Service Transition	Service Validation and Testing	The Supplier shall be responsible for supporting the Authority and Other Suppliers in the Testing of hardware, software and applications as requested by the Authority. If the Authority does require this element of the services, the Authority shall issue a Project Request and the Project Initiation Process set out in Schedule 22 (<i>Change Control Procedure</i>) shall be followed by the Parties.
6.4.7.8	Service Transition	Service Validation and Testing	The Supplier shall support any integration testing where the products, systems or the Services interoperate with Other Suppliers as detailed in the test plan developed by the Authority or Other Suppliers.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.4.7.9	Service Transition	Service Validation and Testing	The Supplier shall ensure that interfaces with external service components are tested as early as possible to de-risk system integration testing.
6.4.7.10	Service Transition	Service Validation and Testing	The Supplier shall provide support as required by the Authority and/or Other Suppliers to create phase/stage Test Plans.
6.4.7.11	Service Transition	Service Validation and Testing	The Supplier shall be responsible for supporting test assurance activities conducted by the Authority and/or Other Suppliers, without adversely impacting the Test Success Criteria or Performance Indicator performance criteria.
6.4.7.12	Service Transition	Service Validation and Testing	Unless otherwise agreed between the Authority and the Supplier, the Supplier shall provide a Non-Live Environment where it is identified as necessary in the Test Strategy/Test Plan and shall ensure that such Non-Live Environment is representative of the live environment.
6.4.7.13	Service Transition	Service Validation and Testing	The Supplier shall ensure that its Non-Live Environments are treated as Deliverables and managed to the required standards.
6.4.7.14	Service Transition	Service Validation and Testing	The Supplier shall make its Non-Live Environment available to the Authority and Other Suppliers, where requested by the Authority.
6.4.7.15	Service Operation	Event Management	The Supplier shall operate its own event management system and ensure it is correctly configured to support the Target Performance Levels.
6.4.7.16	Service Operation	Event Management	The Supplier shall be responsible for the monitoring of the Services to include management of alerts and the investigation and resolution of any Events.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.4.7.17	Service Operation	Event Management	The Supplier shall ensure that the Authority is informed of any corrective action taken to address a potentially service impacting Event and that the relevant records are updated and reported to the Authority within the timescales set out in the Processes.
6.4.7.18	Service Operation	Event Management	The Supplier shall document the Event types and associated Event thresholds which shall be used to measure the availability of the Services in accordance with Paragraph 6.3.1.1.
6.4.7.19	Service Operation	Event Management	The Supplier shall configure its Event management system and associated Devices.
6.4.7.20	Service Operation	Event Management	The Supplier shall configure its Event management system such that it captures the start and end time of availability Events and provides this data to the Authority.
6.5.1.1	Service Operation	Event Management	The Supplier shall ensure that its own Event management system can integrate in near real time with the Authority's Event Management System.
6.5.1.2	Service Operation	Event Management	The Supplier shall be responsible for the investigation and resolution of Events, implementing automated recovery where possible.
6.5.1.3	Service Operation	Incident Management	The Supplier shall deliver Incident Management to the Target Performance Levels and Incident Resolution Deadline as defined in Schedule 3 (<i>Performance Levels</i>).

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.5.1.4	Service Operation	Incident Management	The Supplier shall ensure that the Incident Management process within its own organisation provides an audit trail relating to the management and resolution of Incidents.
6.5.1.5	Service Operation	Incident Management	The Supplier shall support and provide information to the Authority and Other Suppliers to restore normal End To End Services or to provide a Workaround (subject to approval in accordance with the Incident Management Process) during the resolution of Incidents.
6.5.2.1	Service Operation	Incident Management	The Supplier shall acknowledge all Incidents correctly assigned to them and return Incidents to the Authority that have been wrongly assigned in agreement with the Authority.
6.5.2.2	Service Operation	Incident Management	The Supplier shall, following notification of an Incident, schedule and perform resolution activities in accordance with the Processes, specifically Incident Management, contacting End Users where necessary.
6.5.2.4	Service Operation	Incident Management	The Supplier shall update the Incident record with all relevant information within the ITSM Toolset relating to the Incident in accordance with the Incident Management Process.
6.5.2.5	Service Operation	Incident Management	The Supplier shall provide progress updates on all current Incidents in accordance with the Incident Management Process.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.5.2.6	Service Operation	Incident Management	The Supplier shall ensure attendance to any technical Incident management bridge calls and management bridge calls with skilled and experienced staff who understand the service being provided
6.5.2.7	Service Operation	Incident Management	The Supplier shall ensure that where Incident Management information is recorded that the Incident Management System is used to record it and thus either: a)utilise the Incident Management System; or b)operate its own Incident Management system ensuring that it integrates in real time with the Incident Management System.
6.5.2.10	Service Operation	Problem Management	The Supplier shall develop, maintain and provide to the Authority, for inclusion in the Knowledge Management System(s), information on Workarounds, known errors and Problems related to the Services.
6.5.2.11	Service Operation	Problem Management	The Supplier shall resolve problems that have been assigned to them by the Authority in accordance with the relevant Standards.
6.5.3.1	Service Operation	Problem Management	The Supplier shall provide status updates on problem resolution to the Authority.
6.5.3.2	Service Operation	Problem Management	The Supplier shall attend problem reviews as requested by the Authority.
6.5.3.3	Service Operation	Problem Management	The Supplier shall support the Authority in problem analysis as requested including the provision of information relating to problem trends, volumes and resolutions, and

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
			provision of Root Cause Analysis Reports within 10 Working Days of Authority request.
6.5.3.4	Service Operation	Problem Management	The Supplier shall ensure that where Problem Management information is recorded that the Problem Management System is used to record it and thus either it shall: a)utilise the Problem Management System; or b)operate its own Problem Management system ensuring that such system integrates in near-real time with the Problem Management System.
6.5.3.5	Service Operation	Problem Management	The Supplier shall produce Root Cause Analysis Reports for each Problem record that shall include, as a minimum: a)Summary of Problem; b)Timeline and activity by the Supplier including data; c)Root cause analysis; d)Workarounds; e)Recommendations for resolution; and f) Any associated Service Change.
6.5.3.6	Service Operation	Request Fulfilment	The Supplier shall respond to each Service Request within the lead time specified within the Product and Service Catalogue for the relevant Catalogue Item.
6.5.3.7	Service Operation	Request Fulfilment	The Supplier shall promptly notify the Authority of any anticipated failure to fulfil a Service Request within the lead time for the relevant Catalogue Item.
6.5.3.8	Service Operation	Request Fulfilment	The Supplier shall utilise the ITSM Toolset to define the Catalogue Items, create Service Requests and any relevant request fulfilment task.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.5.3.9	Service Operation	Request Fulfilment	In relation to Field Services, the Supplier shall agree with the Authority the specific activities, responsibilities and the service boundaries, as part of the development of the relevant Catalogue Item(s) within the Product and Service Catalogue.
6.5.4.1	Service Operation	Service Desk	The Supplier shall ensure that all contact with End Users is managed and coordinated by the Authority's Service Desk or established routes.
6.5.4.2	Service Operation	Service Desk	The Supplier shall ensure that all communications with End Users, analysis / investigations and recovery actions that have been taken to resolve the ticket are recorded in the appropriate record in the Authority's ITSM Toolset.
6.5.4.3	Service Operation	Service Desk	The Supplier shall ensure that the Supplier Personnel that interact with the Authority's Service Desk are appropriately trained and are capable of working to the relevant standard.
6.5.5.1	Service Operation	Service Desk	The Supplier shall provide all relevant information requested by the Authority to support the onboarding of staff to the Authority's Service Desk, including: 1. Knowledge Base Articles (service desk agent and End User); 2. Minimum data set information; 3. First time fix information; and 4. Material to support service desk agent training on the Services.
6.5.5.2	Service Operation	Service Desk	The Supplier shall provide a suitably staffed service desk capability which is capable of interfacing with the Authority's Service Desk and managing as a minimum Incident(s), Service Requests, complaints and compliments.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.5.5.4	Service Operation	Service Desk	The Supplier shall co-operate with the Authority's Service Desk in the lifecycle management of Incidents.
6.5.5.5	Service Operation	Service Desk	The Supplier will support the Authority in managing any compliment, complaint or escalation in a timely manner.
6.5.5.6	Service Operation	Service Desk	The Supplier will ensure effective prioritisation of complaints and escalations, using an understanding of End User requirements to ensure a timely response, as well as proactively ensuring that lessons are learned to avoid the same complaints and escalations arising in the future.
6.5.5.7	Continual Service Improvement	General	The Supplier shall ensure that at all times, Continual Service Improvement interfaces with all other processes across the service delivery lifecycle.
6.5.5.8	Continual Service Improvement	General	The Supplier shall be responsible for the production, maintenance, provision and implementation of Service Improvement Plans (which for these purposes will have the ITIL definition) for the Services where service improvements have been identified in accordance with Clause 8 (Services Improvement).
6.5.5.9	Continual Service Improvement	General	The Supplier shall support the Authority and Other Suppliers in the implementation of Service Improvement Plans (which for these purposes will have the ITIL definition) where the Supplier has responsibilities for the delivery of components or where requested by the Authority.
6.5.6.1	Continual Service Improvement	General	The Supplier shall suggest new ways of working and propose Continual Service Improvement to the way the service is delivered.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.5.6.4	Continual Service Improvement	General	The Supplier shall ensure that where Continual Service Improvement information is recorded that the Authority's Continual Service Improvement System is used to record it and thus either: a)utilise the Authority's Continual Service Improvement System; or b)operate its own Continual Service Improvement system ensuring that it integrates in near real time with the Authority's Continual Service Improvement System.
6.5.6.5	Service Lifecycle Management	IT Service Management Toolset	The Supplier shall ensure that any Supplier Personnel are fully trained and capable in the use of the Authority's ITSM Toolset for the relevant functions and processes.
6.5.6.6	Service Lifecycle Management	IT Service Management Toolset	The Supplier shall provide and maintain a list of Supplier Personnel who require access to the Authority's ITSM Toolset including the required level of permission.
6.5.6.7	Service Lifecycle Management	IT Service Management Toolset	The Supplier shall ensure that discovery and audit tools for any service components are configured to operational requirements of the Authority's Service Management capabilities e.g. service asset and configuration management and capacity management functions and shall at all times remain compatible with the Authority's ITSM Toolset.
6.5.6.8	Service Lifecycle Management	IT Service Management Toolset	The Supplier shall discuss and agree with the Authority, which Service features can be delivered through the Authority's self-service portal.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.5.6.10	Service Lifecycle Management	IT Service Management Toolset	The Supplier shall create any documentation required by End Users in order to utilise the Services' functions that are agreed to be delivered through the Authority's self-service portal. Such documentation shall be submitted to the Authority for approval in accordance with the relevant Document Approval Procedure or Process.
6.6.1.1	Service Lifecycle Management	IT Service Management Toolset	The Supplier shall ensure that all self-service capabilities that are presented to End Users shall be accessed via the Authority's self-service portal unless otherwise agreed with the Authority.
6.6.1.2	Service Operation	Technical Management	The Supplier shall pro-actively monitor the IT Environment to address actual or potential changes in performance characteristics to ensure compliance with the Target Performance Levels.
6.6.1.3	Service Operation	Technical Management	Where there are any changes to the Authority System or the Services, the Supplier shall inform the Authority with reasonable notice in order to impact assess and mitigate any risks via the Change and Evaluation Management Process.
6.6.1.4	Service Operation	Technical Management	The Supplier must ensure that any equipment, hardware or software used in the provision of the Services will remain in service life support by the manufacturer for the Term.
6.6.1.5	Service Operation	Technical Management	The Supplier must ensure that any equipment, hardware or software used in the provision of the Services that are Transferable Assets are capable (at the time of transfer to the Authority) of remaining in service life support for 2 years after the transfer.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Require ment #	Level 2 Category	Level 3 Category	Requirement
6.7.1.1	Service Operation	Technical Management	Where the manufacturer and/or licensor of hardware, firmware or software used for the provision of the Services has announced or disclosed to the Supplier the withdrawal of support, the Supplier shall promptly notify the Authority.
6.7.1.2	Service Operation	Technical Management	The Supplier shall co-ordinate with the Authority and Other Suppliers of the service components / Configuration Items required for inclusion in builds necessary to ensure continuity of the service.
6.7.1.3	Service Operation	Technical Management	The Supplier shall pro-actively identify and report to the Authority on a monthly basis which Devices are approaching [REDACTED] as well as the associated issues and risks and any actions available to the Parties to eliminate or mitigate such issues or risks. Such report shall be a standing agenda item of the Commercial Board and the Service Review Board unless otherwise agreed.
6.7.1.4	Service Lifecycle Management	Architecture Management	The Supplier shall provide enterprise architecture services for the Supplier System and Services as contracted and ensure these are aligned to Good Industry Practice.
6.7.1.5	Service Lifecycle Management	Architecture Management	The Supplier will store the Documentation on the Authority's Knowledge Management System(s). The Documentation should be managed in line with the Knowledge Management Performance Indicators set out in Schedule 3 (Performance Levels).
6.7.1.6	Service Lifecycle Management	Architecture Management	The Supplier shall update and maintain the Documentation to describe the data, documents and models pertaining to and describing the operation of all real-world components of the Services that provide the Authority with End to End Services (the

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
			“Deployed Architecture”) not less than annually following the Effective Date, and make the updates available to the Authority within one (1) Working Day of the update being approved through the relevant Document Approval Procedure or Process.
6.7.2.1	Service Lifecycle Management	Architecture Management	The Supplier shall provide Deployed Architecture roadmaps for the Services with a three (3) year forecast, describing any change to the Services in order to maintain business operation and submit this to the Authority for Approval through the relevant Document Approval Procedure or Process every 6 months.
6.7.2.2	Service Lifecycle Management	Architecture Management	The Supplier shall perform architecture impact assessment upon the Deployed Architecture for the Services in accordance with the Change and Evaluation Management Process.
6.7.2.3	Service Lifecycle Management	Architecture Management	The Supplier shall ensure that the architecture governance services are aligned to Good Industry Practice.
6.7.2.4	Service Lifecycle Management	Architecture Management	The Supplier shall participate in all relevant architecture governance activities and forums.
6.7.2.5	Service Lifecycle Management	Architecture Management	The Supplier shall ensure that any approved architectural dispensations, waivers, risks, issues and assumptions assigned to the Supplier are managed in alignment to Good Industry Practice.
6.7.2.6	Service Lifecycle Management	Architecture Management	The Supplier shall provide architectural input relation to the Services, providing strategy and direction to the Authority in accordance with Good Industry Practice.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
6.7.2.7	Service Lifecycle Management	Architecture Management	The Supplier shall provide architectural input in relation to the Services, providing strategy and direction to the Authority in accordance with the Standards.
6.7.2.8	General Principles	Collaboration	The Supplier shall co-operate with the Authority and any Other Supplier from time to time by providing: a) reasonable information (including any Documentation); b) advice; and c) reasonable assistance, in connection with the Services to the Authority or any Other Supplier to enable the Authority or any Other Supplier to: d) create and maintain technical or organisational interfaces with the Services, e) support design, delivery and integration of processes and services from multiple suppliers to provide End to End Services, and, on the expiry or termination of this Contract for any reason; and f) enable the timely transition of the Services (or any of them) to the Authority and/or to any Replacement Supplier in accordance with the following collaborative working principles: . proactively leading on, mitigating and contributing to the resolution of problems or issues irrespective of its contractual obligations, acting in accordance with the principle of "fix first, settle later"; . being open, transparent and responsive in sharing relevant and accurate information with the Authority and Other Suppliers; . where reasonable, adopting common working practices, terminology, standards and technology and a collaborative approach to service development and resourcing with the Authority and Other Suppliers;

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Requirement #	Level 2 Category	Level 3 Category	Requirement
			. providing reasonable cooperation, support, information and assistance to the Authority and Other Suppliers in a proactive, transparent and open way and in a spirit of trust and mutual confidence; and . identifying, implementing and capitalising on opportunities to improve deliverables and deliver better solutions and performance throughout the relationship lifecycle.
6.7.2.9	General Principles	Collaboration	Where required, the Supplier shall work with the Authority and Other Suppliers to set out the interdependent relationships in support of delivering the End to End Services including, as a minimum, all the relevant parties' processes (" Operational Interlock Document ").
6.7.2.10	General Principles	Collaboration	The Supplier shall escalate any issues with Other Suppliers, where the Supplier feels it is unable to resolve without intervention from the Authority and or Other Suppliers in the Authority's operating environment to the Authority.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

6.8 WAN Service Management Requirements

The following requirements are specific to this Contract, in addition to the Authority's standard Service Management Requirements (above).

6.8.1 WAN Service Management

The Supplier will have a fully operable service management capability that is measurable and adheres to the WAN Service Management Requirements in this Paragraph 6.8 and the standard Service Management Requirements in Paragraphs 6.1 to 6.7, for the provision of the Services.

6.8.2 Other WAN Supplier management

The Authority requires the Supplier to manage Other WAN Suppliers from time to time.

In all cases, the Authority may request one of three approaches from the Supplier:

1. to novate the relevant Other WAN Supplier's contract;
2. to transfer the relevant services from the Other WAN Supplier to the Supplier in accordance with Clauses 9.8 and 9.9; or
3. 'Agency management' of the Other WAN Supplier.

In all of the above situations, the Supplier shall be required to incorporate the relevant Other WAN Supplier's services into the Supplier's operating model and to manage the relevant Other WAN Supplier against the relevant requirements to achieve the Target Performance Levels and adhering to the requirements set out in 6.1 to 6.7 above.

6.8.3 Connectivity

The Supplier shall provide the WAN Connectivity as a managed service.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

6.8.3.1	WAN Specific Requirement	Connectivity Services	The Supplier shall, regarding Impact Assessments or Changes that involve WAN Connectivity, provide quoting services on-demand and pro-actively for the implementation of WAN Connectivity that include: a) providing the Authority with Impact Assessments reflecting quotes from multiple carriers, ensuring consideration is demonstrably given to the wider market; b) providing the Authority with Impact Assessments that contain the best proposals in the wider market, in terms of functionality, price, reliability, timeframes and ability to integrate with the Authority and Supplier's services; and c) receiving quote requests from the Authority (for changes to existing WAN Connectivity or new WAN Connectivity) and managing the quote requests with the potential Subcontractors.

6.8.4 Maintenance and Support of Authority Assets

6.8.4.1	WAN Specific Requirement	Maintenance and Support Service	Where the Technical Requirements specify that the Supplier shall maintain systems and Authority Assets which form part of the Authority System, the Supplier shall maintain such systems and Authority Assets to ensure the IT Environment performs in accordance with this Contract, including the Target Performance Levels.
6.8.4.2	WAN Specific Requirement	Maintenance and Support Service	The Supplier shall manage spares stock of Devices for the Gateway System subject to such Devices being provided by the Authority, to support Permitted and/or Emergency Maintenance
6.8.4.3	WAN Specific Requirement	Maintenance and Support Service	The Supplier shall keep and update Maintenance Records for the Authority Assets maintained by the Supplier to include: a) Emergency Maintenance; b) Permitted Maintenance; and

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

			c) Asset management including management of spares.

6.8.5 SASE Services (Optional Service)

Subject to implementation (in accordance with Paragraph 7.3 (Optional Services)) of the Transition Requirements) of the relevant SASE Services set out in this Paragraph 0, the Supplier shall provide such Services.

6.8.5.1	SASE Services	Field Services	The Supplier shall provide field engineering services for SD-WAN Edge Devices at Authority Sites, including Emergency Maintenance, in response to: a) Service Incidents raised by the Authority for the SD-WAN Edge Devices ("SASE Service Incidents"); and/or b) Requests.
6.8.5.2	SASE Services	Field Services	The Supplier shall carry out such 'agency management' as is necessary to procure delivery and return of Devices under the Authority's support services subscription(s) with the Other Supplier(s) for SD-WAN Edge Devices.
6.8.5.3	SASE Services	Distributed spares management	The Supplier shall manage nationally distributed spares stock of [REDACTED] SD-WAN Edge Devices (or such other stock holding as may be agreed by the Parties from time to time) subject to such Devices being provided by the Authority, to support Emergency Maintenance in response to SASE Service Incidents or Requests at Authority Sites where no failover Device is installed.

SCHEDULE 2 (Services Description) - ANNEX B (SERVICE MANAGEMENT REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

6.8.6 Not used

6.8.7 Supplier Equipment

6.8.7.1	WAN Specific Requirement	Maintenance and Support Service	The Supplier shall maintain the Supplier Equipment in accordance with Clause 9 to ensure the Services are provided in accordance with this Contract, including the Target Performance Levels.

SCHEDULE 2 - ANNEX C (WAN TRANSITION REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX C – WAN TRANSITION REQUIREMENTS

SCHEDULE 2 (Services Description) - ANNEX C (WAN TRANSITION REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

6 Service Transition

7.1 Transition Planning and Mobilisation

6.1.1.1	The Supplier acknowledges that the purpose of the Implementation Services is to implement the Operational Services, applying the Transition Principles, including: a) Mobilisation of the Supplier's resources, including Supplier Personnel and Sub-contractors; b) Planning and executing the end-to-end processes, procedures, activities, Documentation, Deliverables and governance required for readiness and achievement of cutover to replace the Preceding Services and the Transitional Services with the Operational Services; c) Where applicable, the transfer of assets, personnel, premises, resources and work in progress; d) Coordination of the Implementation Plan with the exit of the Transitional Services; e) Controlled handover of the Operational Services from implementation to operations, including snagging, early life support and assessing the success of the Implementation Services; ("Transition").
6.1.1.2	The Detailed Implementation Plan shall detail all activities, Deliverables and Key Milestones – including aspects related to technical, service, commercial, finance, people, and testing – necessary to achieve a successful Transition.
6.1.1.3	The Supplier shall mobilise an appropriately skilled, qualified, and resourced team, by the Milestone Date indicated in the Implementation Plan.
6.1.1.4	The Supplier shall have a representative who shall have the authority to act on behalf of the Supplier on all matters in connection with the Transition (the "Transition Lead"). The initial Transition Lead shall be the person named as such in Schedule 29 (<i>Key Personnel</i>). Any change to the Transition Lead shall be agreed in accordance with Clause 14 (<i>Supplier Personnel</i>). In addition to

SCHEDULE 2 (Services Description) - ANNEX C (WAN TRANSITION REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

	other requirements of Clause 14 (<i>Supplier Personnel</i>), the Supplier shall ensure that the Transition Lead has experience of delivery in transitions of comparable size and complexity to the Transition.
6.1.1.5	In the event that a Relevant Transfer (or potential Relevant Transfer) is identified, the Supplier shall promptly appoint an HR representative who shall be responsible and accountable for managing on behalf of the Supplier all matters in connection with the Relevant Transfer.
6.1.1.6	The Supplier shall be responsible for the conduct of all circuit surveys including checking the route between the exchange for the relevant Access Circuit and the relevant Authority Site and identifying any potential or necessary Excess Construction Charges.
6.1.1.7	The Supplier shall provide a Documentary Deliverable describing the process(es) for provisioning of Operational Services, including: a) how the Supplier will prepare and present costed options proposals per Authority Site for delivering the WAN Connectivity required in accordance with the Authority Site Specification; b) how the impacts of the costed options will be assessed and presented (e.g. impact on Target Performance Levels, minimum period/notice period for Access Circuits); c) how a variety of approaches will be considered/documented in preparing the costed options (e.g. use of off-net data circuits; alternative connectivity approaches); d) how mitigation options for Excess Construction Costs will be approached and transparently documented; e) the approval process that the Parties will follow to confirm selection and agreement of the relevant costed option per proposal, including the option's impact on the Implementation Plan. When Approved, this Documentary Deliverable shall be the “WAN Services Provisioning Process”.
6.1.1.8	The Supplier shall conduct site readiness surveys in accordance with Paragraphs 2.2.1.8 and 3.2.1.21 of the Technical Requirements and shall request access to the Authority Sites for such surveys with sufficient notice to support the Implementation Plan and having regard to the Authority Site Access Request Process.

SCHEDULE 2 (Services Description) - ANNEX C (WAN TRANSITION REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

6.1.1.9	The Supplier shall provide the Authority with a copy of the Site readiness survey for each Authority Site conducted in accordance with Paragraph 6.1.1.8, including details of any required Remediation.
6.1.1.10	Throughout Transition (including mobilisation), the Supplier shall keep the Authority updated on its resource planning including its actual and forecast recruitment and allocation of Supplier Personnel.
6.1.1.11	The Supplier shall manage Transition risks effectively, including: a) operating an effective Transition risk management plan; b) taking proactive action to resolve all Transition-impacting risks, issues and Defects identified; c) notifying the Authority promptly (and in any case within two (2) Working Days) following a risk, issue or Defect being identified which: (i) may cause a Delay or may adversely impact Projects being delivered by the Supplier and/or other projects (where the Supplier is aware of such other project and the dependencies upon Transition); (ii) could result in “stranded services” (meaning services provided through agreements due to come to an end before a suitable replacement service is provided); or (iii) the Supplier has been or is likely to be unable to resolve; and d) where a risk, issue or Defect may cause a Delay, presenting the Authority with a mitigation plan within five (5) Working Days following that risk issue or Defect being identified, outlining options and a recommendation as to how the impact of the risk, issue or Defect can be mitigated. Note that this requirement does not affect the Supplier’s obligations with regard to Notifiable Defaults and Rectification Plans.
6.1.1.12	In accordance with the timescales in the Implementation Plan, the Supplier shall: a) develop a knowledge transfer plan; and b) evidence the completion of knowledge transfer during testing in accordance with Schedule 14 (Testing Procedures).

SCHEDULE 2 (Services Description) - ANNEX C (WAN TRANSITION REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

6.1.1.13	The Supplier shall provide the Authority with an in-flight project and interim service request report within forty (40) Working Days of the Effective Date. The report will include projects and service requests that were in progress (whether as part of the Preceding Services or other related projects) at the Effective Date and how the projects and service requests will be delivered through to completion by the Supplier under this Contract.
6.1.1.14	The Supplier shall, within the timescales required under the Implementation Plan, provide the Authority with Service Design Packages covering the following Operational Services: a) WAN Connectivity b) Gateway Services c) Core Network Services
6.1.1.15	Throughout Transition, the Supplier shall be responsible for the coordination of the Transition and the Implementation Plan with the exit and/or service transfer arrangements for the Transitional Services.

6.2 Design and Delivery

6.2.1 Design and Delivery General

6.2.1.1	The Supplier shall, unless otherwise agreed with the Authority, gain Approval for the High-Level Design (and/or any update) before it proceeds with any subsequent delivery activities outlined in the Detailed Implementation Plan.
6.2.1.2	The Supplier shall, within the timescales required under the Implementation Plan, provide the Authority with Documentary Deliverables which: (a) describe the IT Environment relating to the Services; (b) detail the Supplier's support responsibilities; (c) include the high-level service design, low level service designs and the product design for each service offerings;

SCHEDULE 2 (Services Description) - ANNEX C (WAN TRANSITION REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

	(d) demonstrate how the Supplier will deliver and operate the Operational Services to meet all relevant obligations under this Contract including how the Operational Services will meet or exceed the Target Performance Levels and meet the reporting requirements of the Service Management Requirements and Schedule 3 (Performance Levels); and (e) provide context, including but not limited to the Deployed Architecture and how it is delivered and how it interfaces with and inter / dependencies of the relevant Operational Services. When Approved, each such Documentary Deliverable shall form the “Service Design Package”.
6.2.1.3	The Supplier shall, within the timescales required under the Implementation Plan, provide the Authority with a Documentary Deliverable which: a) outlines the components, architecture, and functionality of the Supplier Solution; b) provides a narrative of the end-to-end solution; c) describes how the solution interfaces with the Authority’s existing service; and d) how it interfaces with high and low-level technical documentation. When Approved, this Documentary Deliverable shall be the “Solution Design”.
6.2.1.4	Prior to implementing any new Operational Services which may impact the Authority System, the Supplier shall obtain Approval for the relevant Service Design Package(s) (and any update) for the relevant new Operational Services.

SCHEDULE 2 (Services Description) - ANNEX C (WAN TRANSITION REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

7.2.1.6	The Supplier shall follow and comply with the Transition Framework, as amended from time to time, ensuring each Transition is executed in a safe, controlled manner, following a repeatable methodology to manage scope, risk, complexity, and change. The Transition Framework utilises a gated Transition approach which ensures that new, modified, or retired services meet the requirements of the Authority. The Supplier shall provide the relevant documentation, capabilities and resource identified within the Transition Framework.
7.2.1.7	The Supplier shall, no less than two (2) Working Days after cutover of an Authority Site, prepare and release to the Authority for review a “draft post go live report” which includes: a) documentation confirming the completion of the relevant Transition activities at the relevant Authority Site, and that the Supplier has all the requisite credentials, knowledge, and systems expertise to commence the scope of Operational Services at the relevant Authority Site; b) confirmation of the implementation status including final summary of the activities that have been successfully completed by the Supplier at the relevant Authority Site; c) details of service management readiness; d) the operational status of service management processes, tools, monitoring methods, events, and alerts, sufficient to deliver service management capability for Operational Services to commence; e) evidence of satisfaction of the requirements for the issue of a Site Transition Certificate in accordance with the provisions Schedule 13 (Implementation Plan) and Schedule 14 (Testing Procedures) including evidence: (i) of the status and stability of the services following cutover of the relevant Authority Site; and (ii) that there are no Test Issues above those specified in requirement 7.2.1.14; and f) service continuity plans for the relevant Authority Site. Each draft post go live report shall be a Documentary Deliverable to be reviewed and approved in accordance with requirement 7.2.1.9. When Approved, each draft report shall become the “Post Go Live Report” in respect of the relevant Authority Site (each a “Post Go Live Report”).

SCHEDULE 2 (Services Description) - ANNEX C (WAN TRANSITION REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

7.2.1.8	The Authority shall undertake regular cutover to service commencement gate review meetings and notify the Supplier in writing when such review meetings are to occur (the “Cutover Review Board”). In advance of a scheduled Cutover Review Board, the Supplier shall submit any Approved Post Go Live Reports to the Authority for review at such meeting. The Authority shall review the submitted Post Go Live Reports and, where satisfied that a relevant Authority Site can transition into Operational Service, issue a Site Transition Certificate in accordance with Schedule 14 (Testing Procedures). For clarity, the Supplier is required to Achieve any relevant ATP Milestones set out in Schedule 13, including Approval of the cutover to “service commencement gate (Gate 4)” as described within the Transition Framework prior to the issue of any Site Transition Certificate.
7.2.1.9	For the purposes of requirement 7.2.1.7, where a Supplier submits a draft post go live report to the Authority it will be reviewed and Approved or rejected by the Authority within three (3) Working Days of the draft report being received. If the Authority rejects the draft report, it will give its reasons and the Supplier shall address these and re-submit the report within two (2) Working Days of such rejection.

SCHEDULE 2 (Services Description) - ANNEX C (WAN TRANSITION REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

7.2.1.10	The Supplier shall provide the Authority with a draft post go live report within (5) Working Day of the Gateway Services being cutover in accordance with Gateway Services cutover plan. This draft post go live report must include detail of the status and stability of the Gateway Services following Gateway Services cutover, and detail a final summary of the activities that have been successfully completed by the Supplier in respect of the Gateway Services. The draft post go live report is a Documentary Deliverable and will be Approved or rejected by the Authority within five (5) Working Days of being received. Following Approval, the draft report will become the Post Go Live Report for the Gateway Services. If the Authority rejects the draft post go live report, it will give its reasons and the Supplier shall address these and re-submit the report within two (2) Working Days of such rejection.
7.2.1.11	The Supplier shall participate and contribute to post-implementation reviews when requested by the Authority, including when Authority Site migrations are signed off by the Authority as complete.
7.2.1.12	In order to support and in line with the Detailed Implementation Plan the Supplier shall provide the Authority with the following release documentation and details of the following activities: a) release plans; b) cutover plans; c) release packages; and d) implementation and assurance activities associated with the scheduled release.
7.2.1.13	The Supplier shall plan and implement release activity to ensure that there is minimal business disruption to the Authority and the Authority's release management processes are followed.

SCHEDULE 2 (Services Description) - ANNEX C (WAN TRANSITION REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

7.2.1.14	Early life support. a) The Supplier shall provide early life support and address any issues with the relevant Implementation Services during the period from the date each Service or Authority Site is cutover until the relevant Operational Service Commencement Date. b) Implementation Services will not be deemed capable of transition into Operational Service until the relevant services have been implemented in accordance with the Service Design Package, are operationally stable, and there are no Severity Level 1, 2 or 3 Test Issues, and with a Rectification Plan Approved for any Severity Level 4 or 5 Test Issues (if any).
7.2.1.15	The Supplier shall, within the timescales required in the Implementation Plan, provide the Authority with a communications plan which addresses the communication approach for each stakeholder and stakeholder group. The Supplier shall engage with the Authority to identify all relevant stakeholders and stakeholder groups to whom communications shall be required during Transition in order to support a smooth and orderly Transition.
7.2.1.16	Device logistics. The Supplier shall: a) at least 5 Working Days in advance of the scheduled installation date agreed with the Authority for Devices, submit a request in writing to the Authority for delivery of the Devices; b) take delivery of and manage the storage of such Devices; and c) ensure the Devices are conveyed to the Authority Site by the Supplier's field engineer unless otherwise agreed.
7.2.1.17	Following due consultation with and input from the Authority, the Supplier shall propose within the timescales proposed within the Implementation Plan, an Authority Site cutover approach detailing: a) the activities covering the Field Services and any other works for deployment of Operational Services to Authority Sites;

SCHEDULE 2 (Services Description) - ANNEX C (WAN TRANSITION REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

	b) how the Supplier will support the cutover to the Operational Services and formally hand the Operational Services over to the Authority's Service Owner. When Approved, this Documentary Deliverable shall be the "WAN Cutover Approach".
7.2.1.18	Following due consultation with and input from the Authority, the Supplier shall propose within the timescales proposed within the Implementation Plan, a site access request process covering access to Authority Sites and approval to proceed with any works required. When Approved, this Documentary Deliverable shall be the "Authority Site Access Request Process".
7.2.1.19	Within the timescales proposed in the Implementation Plan, the Supplier shall document the procedure for the Parties to follow in respect of Paragraph 7.2.1.15 (Device Logistics) and, subject to Approval of the procedure, the Parties shall follow such procedure whenever Devices are required for installation.
7.2.1.20	The Supplier shall undertake the installation and deployment of Devices at the Authority Sites as specified in the Authority Site Specification, in accordance with Paragraph 2.2.1 of the Technical Requirements.
7.2.1.21	The Supplier shall implement the Gateway Services by taking over the management and delivery of the equivalent Transitional Services, including taking over the Gateway System on an "as-is" basis.
7.2.1.22	During Service Design, the Parties shall review the Performance Indicator for Capacity Management. Following such review, the Authority may, on giving the Supplier four weeks' notice, replace the measure of the Capacity Management Performance Indicator with a different measure of Capacity Management. The Supplier shall not be entitled to object to any changes made by the Authority under this Paragraph 7.2.1.22, or increase the Service Charges as a result of such changes, provided that the principle purpose of the change is to reflect the Authority's business requirements and priorities at the time and the change reflects industry standards.

6.2.2 Transition General

6.2.2.1	The Supplier shall, on a weekly basis, report to the Authority with a project status report on the progress of the Transition and the Deliverables. This shall include as a minimum, the planned and forecast Milestone Dates

SCHEDULE 2 (Services Description) - ANNEX C (WAN TRANSITION REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

	for Transition, and the dates for completion of the Deliverables and such other information as the Authority may request.

6.2.3 Service Continuity

6.2.3.1	The Supplier shall provide the Transitional Services in accordance with Schedule 34 (Transitional Services).
6.2.3.2	The Supplier shall ensure that the Operational Services interface with the Transitional Services until the Transitional Services have been replaced and/or decommissioned.

6.3 Optional Services

6.3.1.1	The Supplier shall develop the Optional Services Implementation Plan under the Change Control Procedure, subject to Paragraph 6.3.1.3, following receipt of the Authority's notice(s) pursuant to Clause 5.10.
6.3.1.2	Documentary Deliverables required under the Optional Services Implementation Plan shall include updated versions of: a) the High Level Design; b) the relevant Service Design Package; c) relevant Low Level Designs; and d) such other updated documents as may be required for the relevant Optional Services.
6.3.1.3	Following receipt of the Authority's notice pursuant to Clause 5.10 for any of the Optional Services, the relevant Impact Assessment (as defined in Schedule 22 (<i>Change Control Procedure</i>)) shall include: a) the impact on the Optional Services Implementation Plan;

SCHEDULE 2 (Services Description) - ANNEX C (WAN TRANSITION REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

	b) the impact on reports required under this Contract, including the Performance Monitoring Report (as defined in Schedule 3 (<i>Performance Levels</i>); and c) the results of the Supplier's verification activity for any relevant Allowable Assumption, including whether the Allowable Assumption is accurate or whether the Optional Services Implementation Plan requires adjustment.

SCHEDULE 2 - ANNEX D (WAN SOCIAL VALUE REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX D – SOCIAL VALUE REQUIREMENTS

SCHEDULE 2 (Services Description) - ANNEX D (WAN SOCIAL VALUE REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

1 BACKGROUND

- 1.1 In December 2020, HM Government published 'The Social Value Model' in conjunction with 'Guide to Using the Social Value Model' which in combination set out the approach to be taken by government authorities to supporting social value, including themes, policy outcomes, benefits, effective measures, contract management and reporting.
(<https://www.gov.uk/government/publications/procurement-policy-note-0620-taking-account-of-social-value-in-the-award-of-central-government-contracts>)
- 1.2 The Authority expects its suppliers and sub-contractors to support the activities set out in 'The Social Value Model' and its associated guidance, including the Supplier's and Sub-contractors' compliance with the requirements set out in this Annex D.
- 1.3 The Supplier acknowledges that HM Government may further develop and change its social value model, and the Authority may have additional requirements in relation to social value. The Authority expects that the Supplier and Sub-contractors will comply with such reasonable social value requirements as the Authority may notify to the Supplier from time to time. Any necessary changes to the Contract shall be enacted via the Change Control Procedure.

2 THEMES, OUTCOMES AND BENEFITS

- 2.1 The Supplier shall support the following social value themes, policy outcomes and benefits:

Table 1 – Social value themes, outcomes and benefits selected from the social value model

Theme	Policy outcomes	Benefits
Tackling economic inequality	Create new businesses, new jobs and new skills	MAC 2.2: Create employment and training opportunities particularly for those who face barriers to employment and/or who are located in deprived areas and/or can be supported to avoid reoffending and industries with known skills shortages or in high growth sectors.

SCHEDULE 2 (Services Description) - ANNEX D (WAN SOCIAL VALUE REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Fighting climate change	Effective stewardship of the environment	MAC 4.1: Deliver additional environmental benefits in the performance of the contract including working towards net zero greenhouse gas emissions.

3 SOCIAL VALUE DELIVERY PLAN

- 3.1 Within sixty (60) days of the Commencement Date, the Supplier must provide to the Authority a fully complete, up-to-date, timed project plan and process for delivering social value benefits (the '**Social Value Delivery Plan**') for the Authority to agree.
- 3.2 The Social Value Delivery Plan must contain information at the level of detail necessary to manage and deliver:
 - 3.2.1 social value commitments included in the Supplier's tender;
 - 3.2.2 monitoring, measuring and reporting on social value benefits (including those listed in Paragraph 2), commitments and impacts;
 - 3.2.3 timed actions;
 - 3.2.4 reporting including metrics, targets (to be assigned to metrics wherever possible), tools and processes to gather and report data;
 - 3.2.5 feedback and improvement;
 - 3.2.6 transparency;
 - 3.2.7 influencing of stakeholders and communities through the Contract Period to support the policy outcomes (e.g. engagement, co-design/creation, training and education, partnering/collaborating, volunteering).
- 3.3 The Social Value Delivery Plan will identify the Supplier Personnel responsible for its delivery.
- 3.4 Following receipt of the Social Value Delivery Plan from the Supplier, the Parties shall use reasonable endeavours to agree any amendments reasonably required for Authority to accept the Social Value Delivery Plan. If the Parties are unable to agree the Social Value Delivery Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

SCHEDULE 2 (Services Description) - ANNEX D (WAN SOCIAL VALUE REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

3.5 The Supplier shall keep the Social Value Delivery Plan under review at least annually and as otherwise directed by any Board (as described in Schedule 21 (Governance)) and will propose changes where necessary to improve outcomes.

4 PERFORMANCE MONITORING AND REPORTING

4.1 The Supplier shall monitor its performance against the Social Value Delivery Plan and report to the Authority on such performance quarterly, in a format reasonably specified by the Authority from time to time.

4.2 The Supplier's reports on social value delivery will be reviewed as a regular contract management activity, including in scope of relevant Board(s) (as described in Schedule 21 (Governance)).

4.3 The Supplier's reports on social value delivery must include the reporting metrics used by HM Government to monitor progress against the relevant policy outcomes, including those listed in Table 2 below.

Table 2 – Reporting metrics for progress on policy outcomes (from social value model)

Policy outcomes	Reporting metrics
Create new businesses, new jobs and new skills	• Number of full-time equivalent (FTE) employment opportunities created under the Contract, by UK region. • Number of apprenticeship opportunities (level 2, 3, and 4+) created or retained under the Contract, by UK region. • Number of training opportunities (level 2, 3, and 4+) created or retained under the Contract, other than apprentices, by UK region. • Number of people-hours of learning interventions delivered under the Contract, by UK region. • Number of sustainable employment opportunities provided to prison leavers under the contract, by UK region • Number of employed prison leavers who additionally receive learning, upskilling and reskilling in their first 6 months of employment to support them in continued/future employability opportunities, under the contract, by UK region • Proportion of employed prison leavers that are subsequently retained within the Contractor organisation or associated supply chain, under the contract, by UK Region

SCHEDULE 2 (Services Description) - ANNEX D (WAN SOCIAL VALUE REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Effective stewardship of the environment	• Number of people-hours spent protecting and improving the environment under the Contract, by UK region. • Number of green spaces created under the Contract, by UK region. • Annual: ○ Reduction in emissions of greenhouse gases arising from the performance of the Contract, measured in metric tonnes carbon dioxide equivalents (MTCDE). ○ Reduction in water use arising from the performance of the Contract, measured in litres. ○ Reduction in waste to landfill arising from the performance of the Contract, measured in metric tonnes.

4.4 Performance against the targets in the Social Value Delivery Plan will be evaluated using the following scores:

Table 3 – Scores for evaluating social value targets

Good	The Supplier is meeting or exceeding the target set out within the Social Value Delivery Plan.
Approaching target	The Supplier is close to meeting the targets are set out within the Social Value Delivery Plan.
Requires improvement	The performance of the Supplier is below that of the target set out within the Social Value Delivery Plan, but Supplier has identified and committed to and/or is progressing steps to improve its performance.
Inadequate	The performance of the Supplier is significantly below that of the target set out within the Social Value Delivery Plan.

4.5 The Social Value Delivery Plan will set out how the Social Value PI will be calculated based on evaluation of targets in accordance with paragraph 4.4, using the following template:

Table 4 – Template for evaluation of specific reporting metrics

Reporti ng metric	Delivery period	Performance thresholds				Actual Delivery	% Delivery	Rating
		Good	Approaching target	Requires improvement	Inadequate			
[Insert]	Q [insert] [Year]	[Threshold]	[Threshold]	[Threshold]	[Threshold]	[Insert]	[Actual/	[Insert]

SCHEDULE 2 (Services Description) - ANNEX D (WAN SOCIAL VALUE REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

							<i>Good x100]</i>	
<i>[Insert]</i>	<i>Q [insert] [Year]</i>	<i>[Threshold]</i>	<i>[Threshold]</i>	<i>[Threshold]</i>	<i>[Threshold]</i>	<i>[Insert]</i>	<i>[Actual/ Good x100]</i>	<i>[Insert]</i>
<i>[Insert]</i>	<i>Q [insert] [Year]</i>	<i>[Threshold]</i>	<i>[Threshold]</i>	<i>[Threshold]</i>	<i>[Threshold]</i>	<i>[Insert]</i>	<i>[Actual/ Good x100]</i>	<i>[Insert]</i>
<i>[Insert]</i>	<i>Q [insert] [Year]</i>	<i>[Threshold]</i>	<i>[Threshold]</i>	<i>[Threshold]</i>	<i>[Threshold]</i>	<i>[Insert]</i>	<i>[Actual/ Good x100]</i>	<i>[Insert]</i>

4.6 The Authority may publish social value performance metrics relating to the Contract from time to time, including in accordance with HM Government practice at the time.

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SCHEDULE 3
PERFORMANCE LEVELS

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Schedule 3 (*Performance Levels*)

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

“Available”	has the meaning given in Paragraph 1.1 of Part B of Annex 1 to this Schedule 3;
“In-Scope Services”	means the Services set out in Paragraph 2 of Part B of Annex 1 to this Schedule 3 and shall be Available 24 / 7 / 365;
“On Hold Time”	means the period of time that the status of an Incident, Service Request or task is suspended (stop the clock) as further set out in the Processes. Examples of when this might occur include: (a) provision of information or action from the Authority or Other Supplier without which the Supplier is unable to diagnose or resolve an Incident, Service Request or task; and (b) End User unavailable to test and/or confirm whether the Service Incident or Security Incident has been resolved or whether the Catalogue Item(s) has/have been fulfilled;
“Performance Monitoring Report”	has the meaning given in Paragraph 1.2 of Part B to this Schedule 3;
“Repeat KPI Failure”	has the meaning given in Paragraph 3.1 of Part A to this Schedule 3;
“Resolution”	means in relation to a Service Incident and/or Security Incident action has been taken and (1) has repaired the cause(s) of a Service Incident and/or Security Incident or (2) implemented a Workaround to the satisfaction of the Authority, and “Resolved” shall be construed accordingly;
“Resolution Deadline”	means the deadline for Resolution in accordance with the following paragraphs of Part B of Annex 1 to this Schedule 3: – for Service Incidents, Paragraph 3.10; and

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

– for Security Incidents, Paragraph 4.4;

“Resolution Time”	resolution time of a Service Incident and/or a Security Incident is the period from the time that the incident is reported to the Supplier to the point of its Resolution;
“Service Downtime”	means any period of time during which any of the Services are Unavailable;
“Service Hours”	means the periods during which the Supplier shall provide Operational Services and make them Available and so as to meet or exceed the Target Performance Level for each Performance Indicator. The Service Hours for each Authority Site are stated in the Authority Site List and will be either: • 24x7 (inc Bank Holidays); or • 08:00 – 21:30 UK Time Monday to Friday (excluding a Saturday, Sunday or a public holiday in England and Wales);
“Service Incident”	a reported occurrence of an unplanned interruption to or reduction in the quality of any part of the Services in accordance with the Authority Requirements or the Performance Indicators;
“Service Review Board”	the regular meetings between the Supplier and the Authority to manage and review the Supplier's performance under this Contract, as further described in Paragraph 1.10 of Part B to this Schedule 3;
“Security Incident”	means the act of breaching an explicit or implied security policy;
“Unavailable”	in relation to the IT Environment or the Services, that the IT Environment or the Services are not Available; and “Unavailability” shall be construed accordingly; and
“VIP Site”	has the meaning given in Paragraph 3.5 of Annex 1 to this Schedule 3.

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Part A: Performance Indicators and Service Credits**1 PERFORMANCE INDICATORS**

- 1.1 Annex 1 to this Schedule 3 sets out the Key Performance Indicators and Subsidiary Performance Indicators which the Parties have agreed shall be used to measure the performance of the Services and Social Value by the Supplier.
- 1.2 The Supplier's performance against each Performance Indicator shall be monitored and reported by the Parties in accordance with Part B (*Performance Monitoring*) of this Schedule 3.
- 1.3 Service Points, and therefore Service Credits, shall accrue for any KPI Failure and shall be calculated in accordance with Paragraphs 2, 3 and 5.

2 SERVICE POINTS

- 2.1 If the level of performance of the Supplier during a Service Period achieves the Target Performance Level in respect of a Key Performance Indicator, no Service Points shall accrue to the Supplier in respect of that Key Performance Indicator.
- 2.2 If the level of performance of the Supplier during a Service Period is below the Target Performance Level in respect of a Key Performance Indicator, Service Points shall accrue to the Supplier in respect of that Key Performance Indicator as set out in Paragraphs 2.3 and 2.4.
- 2.3 The number of Service Points that shall accrue to the Supplier in respect of a KPI Failure shall be the applicable number as set out in Annex 1 depending on whether the KPI Failure is a Minor KPI Failure, a Serious KPI Failure or a Severe KPI Failure, or the KPI Failure breaches the relevant KPI Service Threshold, unless the KPI Failure is a Repeat KPI Failure when the provisions of Paragraph 3.2 shall apply.
- 2.4 In calculating Service Points in respect of KPI-01a, KPI-01b, KPI-01c, KPI-02, KPI-04 and KPI-05, if the level of performance of the Supplier falls below the KPI Service Threshold in respect of a Key Performance Indicator, Service Points shall continue to accrue in respect of the relevant Key Performance Indicator as set out in Annex 1.

3 REPEAT KPI FAILURES AND RELATED KPI FAILURES**Repeat KPI Failures**

- 3.1 If a KPI Failure occurs in any two consecutive Measurement Periods:
 - 3.1.1 in respect of the KPI "Availability: WAN Connectivity", at the same Authority Site; or
 - 3.1.2 otherwise, in respect of the same Key Performance Indicator;

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- the second and any subsequent such KPI Failure shall be a “**Repeat KPI Failure**”.
- 3.2 The number of Service Points that shall accrue to the Supplier in respect of a KPI Failure that is a Repeat KPI Failure shall be calculated as follows:

SP = P x 2

where:

- SP** = the number of Service Points that shall accrue for the Repeat KPI Failure; and
- P** = the applicable number of Service Points for that KPI Failure as set out in Annex 1 depending on whether the Repeat KPI Failure is a Minor KPI Failure, a Serious KPI Failure, a Severe KPI Failure or a failure to meet the KPI Service Threshold.

Table 1:Worked example for information only based on the following Service Points regime for KPI-02 – Incident Resolution Times: Severity 1 Incidents

KPI-02 Severity 1 Levels		Service Points
Target Performance Level:	0 minutes late	0
Minor KPI Failure:	>1 minute; up to 2 hours late	from 22 to 45
Serious KPI Failure:	>2 hours late; up to 4 hours late	from 46 to 75
Severe KPI Failure:	>4 hours late; up to 10 hours late	from 76 to 255
KPI Service Threshold:	>10 hours late	256

Example 1:

If the Supplier resolves a Severity 1 Service Incident between one minute late and 119 minutes’ late within a given Measurement Period, it will incur a Minor KPI Failure for “Incident Resolution Times: Severity 1 Incidents” in that Measurement Period and accordingly accrue 22 Service Points and then 1 additional Service Point per five minutes’ late.

If, in the next Measurement Period, the Supplier resolves a Severity 1 Service Incident between 120 minutes’ late and 239 minutes’ late, it will incur a Serious KPI Failure and would have accrued 46 Service Points and then 1 additional Service Point per 4 minutes but for the failure being a Repeat KPI Failure, which results in the Service Points being doubled and therefore the

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Supplier will incur 92 Service Points and then 2 additional Service Points per 4 minutes for the failure (i.e. $SP = 46 \times 2 + 1 \times 2$ per additional 4 minutes).

If in the next Measurement Period the Supplier resolves a Severity 1 Service Incident between one minute late and 119 minutes' late, the Supplier will incur 44 Service Points and then 2 additional Service Points per 5 minutes.

Example 2:

If the Supplier resolves a Severity 1 Service Incident between 120 minutes late and 239 minutes' late in a given Measurement Period, it will incur a Serious KPI Failure for Incident Resolution Times: Severity 1 Incidents in that Measurement Period and accordingly accrue 46 Service Points and then 1 additional Service Point per 4 minutes.

If, in the next Measurement Period, it resolves a Severity 1 Service Incident between 1 minute late and 119 minutes late it will incur a Minor KPI Failure and accordingly accrue 22 Service Points and then 1 additional Service Point per 5 minutes. However, as the failure is a Repeat KPI Failure, this amount is doubled and so the Supplier will incur 44 Service Points and then 2 additional Service Points per 5 minutes for the failure (i.e. $SP = 22 \times 2 + 1 \times 2$ per additional 5 minutes).

If in the next Measurement Period, it resolves a Severity 1 Service Incident between 1 minute late and 119 minutes late the Supplier will incur 44 Service Points and then 2 additional Service Points per 5 minutes.

Related KPI Failures

3.3 Not used.

Material PI Failures

3.4 Where a Subsidiary Performance Indicator measures items due within a Service Period (e.g. Project Proposals; Root Cause Analysis Reports):

- 3.4.1 it shall be considered to have been measured as a single Subsidiary Performance Indicator when one or more of the relevant items were due in the Service Period;
- 3.4.2 it shall not be considered to have been measured in any Service Period when no relevant items were due.

Example 1

If two Project Proposals were due within the Service Period, 'Proposal Turnaround' will have been measured as a single Subsidiary Performance Indicator for the purposes of calculating the number of Subsidiary Performance Indicators that were measured in the Service Period; even though the Performance Indicator will apply to each Project Proposal.

Example 2

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

If no Root Cause Analysis Reports were due in the Service Period, then the 'Root Cause Analysis' Performance Indicator will not be measured. The total number of Subsidiary Performance Indicators measured will therefore not include 'Root Cause Analysis' for that Service Period.

4 PERMITTED MAINTENANCE

- 4.1 The Supplier shall be allowed to book Service Downtime for Permitted Maintenance in accordance with the Authority's Change and Evaluation Management Process, such Service Downtime to take place between the hours and on the day specified in the Maintenance Schedule and/or relevant RFC unless otherwise agreed in writing with the Authority.

5 SERVICE CREDITS

- 5.1 Schedule 15 (*Charges and Invoicing*) sets out the mechanism by which Service Points shall be converted into Service Credits.
- 5.2 The Supplier shall use the Performance Monitoring Reports provided pursuant to Part B of this Schedule 3, among other things, to verify the calculation and accuracy of the Service Credits (if any) applicable to each Service Period.
- 5.3 Notwithstanding the provisions of Schedule 15 (*Charges and Invoicing*), and at the Authority's discretion, the Parties may agree benefits to be delivered by the Supplier in substitution for the payment of Service Credits, such benefits to be of at least equivalent value to the Service Credits that would otherwise be payable. If benefits are substituted for Service Credits as agreed by the Parties, the value of the Service Credits that have been substituted shall be taken into account for the purposes of calculating whether the Service Credit Cap has been reached.

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Part B: Performance Monitoring**1 PERFORMANCE MONITORING AND PERFORMANCE REVIEW**

- 1.1 The performance of the Supplier against each of the Performance Indicators shall be measured as follows:
- (a) the Social Value PI (SPI-01) shall be measured in accordance with the Social Value Delivery Plan;
 - (b) the Vulnerability Management PI (SPI-08) shall be measured by the Supplier;
 - (c) all other Performance Indicators shall be measured in the ITSM Toolset in accordance with the Processes, unless otherwise agreed by the Authority.
- 1.2 During each Service Period, the Parties shall:
- (a) update and maintain all records in the ITSM Toolset relevant to the Performance Indicators, in accordance with the Authority's processes relating to the ITSM Toolset; and
 - (b) work together in accordance with the Authority's performance reporting process to produce a report which summarises performance by the Supplier against each of the Performance Indicators as more particularly described in Paragraph 1.6 (the "Performance Monitoring Report").
- 1.3 Within ten (10) Working Days of the end of each Service Period, the Supplier shall, upon request from the Authority in accordance with Paragraph 1.7, provide a report to the Authority Representative which summarises the Supplier's performance over the relevant Service Period as more particularly described in Paragraph 1.7 (the "**Balanced Scorecard Report**").
- 1.4 The Supplier shall review the performance achieved for all Performance Indicators, Response Times and Resolution Deadlines as part of its continual service improvement responsibilities and report periodically (at least quarterly) to the Authority on them as part of the Performance Monitoring Report.
- 1.5 In order to monitor and continuously improve the services it receives, the Authority may undertake satisfaction surveys in respect of End Users or various groups of End Users, and any results relevant to the Services will be summarised in the Performance Monitoring Report.

Performance Monitoring Report

- 1.6 The Performance Monitoring Report shall be in such format as reasonably decided by the Authority and contain, as a minimum, the following:

Information in respect of the Service Period just ended

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (a) executive summary;
- (b) Capacity Report;
- (c) for each Key Performance Indicator and Subsidiary Performance Indicator, the actual performance achieved over the Service Period;
- (d) a summary of all Performance Failures that occurred during the Service Period;
- (e) the performance level of each Performance Indicator as defined in Table 2 and Table 3 in Part A of Annex 1 (*i.e.* "Target Performance Level", "Minor KPI Failure", "Severe KPI Failure", "KPI Service Threshold", "Service Threshold");
- (f) which Performance Failures remain outstanding and progress in resolving them;
- (g) for any Material KPI Failures or Material PI Failures occurring during the Service Period the cause of the relevant KPI Failure or PI Failure and the action being taken to reduce the likelihood of recurrence;
- (h) for any Repeat KPI Failures, actions taken to resolve the underlying cause and prevent recurrence;
- (i) the number of Service Points awarded in respect of each KPI Failure;
- (j) the Service Credits to be applied, indicating the KPI Failure(s) to which the Service Credits relate;
- (k) any relevant matters arising from satisfaction surveys;
- (l) the status of any outstanding Rectification Plan processes, including:
 - whether or not a Rectification Plan has been agreed; and
 - where a Rectification Plan has been agreed, a summary of the Supplier's progress in implementing that Rectification Plan;
- (m) the conduct and performance of any agreed periodic tests that have occurred, such as the annual failover test of the Service Continuity Plan; and
- (n) relevant particulars of any aspects of the Supplier's performance which fail to meet the requirements of this Contract;
- (o) review of Service Management risks that are emerging, new and ongoing including the mitigating activity;

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (p) Analysis of trends and patterns in IT performance including as a minimum Availability, Capacity, Event, Incidents, Problems, Service Change, and Performance Indicators to cover the last 6 months of data;
- (q) Incident and Problem Management including summary information on Severity 1 and Severity 2 Incidents, any common factors, resolution and associated Problems;
- (r) Sustainability report that sets out the Carbon Dioxide, Methane and Nitrous Oxide emission on a rolling monthly basis;
- (s) Security report as described in Paragraph 16.12 of Schedule 5 (*Security Management*);
- (t) such other details and/or sections for Supplier input as the Authority may reasonably decide from time to time.

Information in respect of previous Service Periods

- (u) for each Key Performance Indicator and Subsidiary Performance Indicator, the actual performance achieved over the previous 12 months;
- (v) a rolling total of the number of Performance Failures that have occurred over the past six Service Periods;
- (w) the amount of Service Credits that have been incurred by the Supplier over the past six Service Periods;
- (x) the conduct and performance of any agreed periodic tests that have occurred in such Service Period such as the annual failover test of the Service Continuity Plan.

Information in respect of the next Quarter

- (y) any scheduled Service Downtime for Permitted Maintenance and Updates that has been requested by the Supplier and/or agreed between the Parties for the next Quarter;
- (z) at least quarterly, continuous service improvement opportunities in respect of performance achieved; and
- (aa) the updated Capacity Plan.

Balanced Scorecard Report

- 1.7 The Authority may at any time during the Term, upon 30 days' notice, request the Supplier to implement the Balanced Scorecard Report requirements of Paragraphs 1.3 and 1.8, and until such notice is made the Supplier shall not be required to perform those requirements.

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 1.8 Upon request from the Authority in accordance with Paragraph 1.7, the Balanced Scorecard Report shall be presented by the Supplier in such format as agreed between the Parties from time to time and, as a minimum, shall contain a high level summary of the Supplier's performance over the relevant Service Period, including details of the following:
- (a) financial indicators;
 - (b) the Target Performance Levels achieved;
 - (c) behavioural indicators;
 - (d) performance against its obligation to pay its Sub-contractors within thirty (30) days of receipt of an undisputed invoice;
 - (e) performance against its obligation to pay its Unconnected Sub-contractors within sixty (60) days of receipt of an invoice;
 - (f) Milestone trend chart, showing performance of the overall programme;
 - (g) sustainability indicators, for example net zero carbon, waste minimisation or performance to support a circular economy; and
 - (h) Social Value.
- 1.9 The Performance Monitoring Report – and, if requested by the Authority under Paragraph 1.7, the Balanced Scorecard Report – shall be reviewed and their contents agreed by the Parties at the next Service Review Board held in accordance with Paragraph 1.10.
- 1.10 The Parties shall attend meetings on a monthly basis (unless otherwise agreed) to review the Performance Monitoring Reports and, if requested by the Authority under Paragraph 1.7, the Balanced Scorecard Reports (the **"Service Review Board"**). The Service Review Board shall (unless otherwise agreed):
- (a) take place within 5 Working Days of the Performance Monitoring Report being issued to the Authority Representative by the Supplier;
 - (b) take place at such location and time (within normal business hours) as the Authority shall reasonably require (unless otherwise agreed in advance); and
 - (c) be attended by the Supplier Representative and the Authority Representative.
- 1.11 The Authority shall be entitled to raise any additional questions and/or request any further information from the Supplier regarding any KPI Failure and/or PI Failure or any other service impacting event.
- 1.12 The information to be provided by the Supplier in accordance with Paragraphs 1.6 and 1.8 shall constitute Supporting Documentation and, in accordance with

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Paragraph 1.5 of Part E of Schedule 15 (*Charges and Invoicing*), must accompany the relevant invoice.

- 1.13 Following commencement of any Optional Service in accordance with Clause 5.12, all subsequent Performance Monitoring Reports will include impact of the relevant Optional Service on the Performance Indicators.

2 PERFORMANCE RECORDS

- 2.1 In addition to any other Management Information and record keeping requirements set out in this Contract, the Supplier shall keep appropriate documents and records (including Supplier System logs, staff records, timesheets, training programmes, staff training records, goods received documentation, supplier accreditation records, complaints received etc) in relation to the Services being delivered. The records and documents of the Supplier shall be available for inspection by the Authority and/or its nominee at any reasonable time and the Authority and/or its nominee may make copies of any such records and documents. Where the Authority's nominee is a direct competitor of the Supplier, the Authority shall, at the written request of the Supplier, require the nominee to enter into a confidentiality agreement with the Supplier in a form reasonably specified by the Supplier.
- 2.2 In addition to the requirement in Paragraph 2.1 to maintain appropriate documents and records, the Supplier shall provide to the Authority such supporting documentation as the Authority may reasonably require in order to verify the level of the performance of the Supplier both before and after each Operational Service Commencement Date and the calculations of the amount of Service Credits for any specified period.
- 2.3 The Supplier shall ensure that the Balanced Scorecard Report (as well as historic Balanced Scorecard Reports) and any variations or amendments thereto, any reports and summaries produced in accordance with this Schedule and any other document or record reasonably required by the Authority are available to the Authority in a format reasonably agreed.

3 PERFORMANCE VERIFICATION

- 3.1 The Authority reserves the right to verify the Availability of the IT Environment and/or the Services and the Supplier's performance under this Contract against the Performance Indicators including by sending test transactions through the IT Environment or alerts, log verification and manual checks.

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Annex 1: Key Performance Indicators and Subsidiary Performance Indicators**Part A: Key Performance Indicators and Subsidiary Performance Indicators Tables**

The Key Performance Indicators and Subsidiary Performance Indicators that shall apply to the Operational Services and the Performance Indicator relating to Social Value are set out below:

1 Key Performance Indicators

1.1 The Key Performance Indicators in Table 2 shall apply to all Operational Services.

Table 2 – KPIs for all Operational Services

No.	Key Performance Indicator title	Definition	Frequency of measurement	Performance levels	Service Points	Publishable Performance Information
KPI-01a	Availability: WAN Connectivity	See Paragraph 2.1 of Part B of this Annex 1	Monthly	See Paragraph 2.4 of Part B of this Annex 1	1 Service Point for each 0.01% below the Target Performance Level	Yes
KPI-01b	Availability: Gateway System	See Paragraph 2.1 of Part B of this Annex 1	Monthly	Target Performance Level: 99.99% Minor KPI Failure: 99.7% – 99.98% Serious KPI Failure: 99.5% – 99.69% Severe KPI Failure: 99% – 99.49%	1 Service Point for each 0.01% below the Target Performance Level	Yes

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

No.	Key Performance Indicator title	Definition	Frequency of measurement	Performance levels	Service Points	Publishable Performance Information
				KPI Service Threshold: Below 99%		
KPI-02	Incident Resolution Times: Severity 1 Service Incidents & Severity 2 Service Incidents	See Paragraph 3.11 of Part B of this Annex 1	Monthly	See Paragraph 3.12 of Part B of this Annex 1	Paragraph 3.13 of Part B of this Annex 1 and Table 8 describe the Service Points for this KPI and the methodology for calculating Service Points.	Yes
KPI-03	Incident Resolution Times: Severity 3 Service Incidents	See Paragraph 3.11 of Part B of this Annex 1	Monthly	See Paragraph 3.12 of Part B of this Annex 1	Paragraph 3.13 of Part B of this Annex 1 and Table 8 describe the Service Points for this KPI and the methodology for calculating Service Points.	Yes
KPI-04	Security Incident Response Time	See Paragraph 4.5 of Part B	Monthly	See Paragraph 4.6 of Part B of this Annex 1 and Table 9.	Paragraph 4.7 of Part B of this Annex 1 and Table 10 describe the Service Points	No

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

No.	Key Performance Indicator title	Definition	Frequency of measurement	Performance levels	Service Points	Publishable Performance Information
		of this Annex 1			for this KPI and the methodology for calculating Service Points.	
KPI-05	Security Incident Resolution Time	See Paragraph 4.8 of Part B of this Annex 1	Monthly	See Paragraph 4.9 and Table 11 of Part B of this Annex 1	Paragraph 4.10 of Part B of Annex 1 and Table 12 describe the Service Points for this KPI and the methodology for calculating Service Points.	No
KPI-06	Change Management	See Paragraph 5.1 of Part B of this Annex 1	Monthly	See Table 13 at Paragraph 5.3 of Part B of this Annex 1	Target Performance Level: 0 Minor KPI Failure: 10 Serious KPI Failure: 20 Severe KPI Failure: 30 KPI Service Threshold: see Paragraph 5.4 of Part B of Annex 1 for the Service Points allocation and methodology for calculating Service Points.	Yes

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

No.	Key Performance Indicator title	Definition	Frequency of measurement	Performance levels	Service Points	Publishable Performance Information
KPI-07	Service Request Fulfilment	See Paragraph 6.1 of Part B of this Annex 1	Monthly	See Table 14 in Paragraph 6.3 of Part B of this Annex 1	Target Performance Level: 0 Minor KPI Failure: 10 Serious KPI Failure: 20 Severe KPI Failure: 30 KPI Service Threshold: see Paragraph 6.4 of Part B of Annex 1 for the Service Points allocation and methodology for calculating Service Points	Yes
KPI-08	Knowledge Management	See Paragraph 7.2 of Part B of this Annex 1	Monthly	See Table 15 in Paragraph 7.3 of Part B of this Annex 1	Target Performance Level: 0 Minor KPI Failure: 10 Serious KPI Failure: 20 Severe KPI Failure: 30 KPI Service Threshold: see Paragraph 7.4 of Part B of Annex 1 for the Service Points allocation and methodology for calculating	Yes

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

No.	Key Performance Indicator title	Definition	Frequency of measurement	Performance levels	Service Points	Publishable Performance Information
					Service Points	

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

2 Subsidiary Performance Indicators

2.1 The Subsidiary PIs in Table 3 shall apply to all Operational Services and Social Value.

Table 3 – Subsidiary PIs for all Operational Services and Social Value

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Performance levels	Publishable Performance Information
SPI-01	Social Value Delivery (“ Social Value PI ”)	See the Social Value Delivery Plan (“ SVDP ”)	Quarterly	Target Performance Level: “Good” (as defined in the SVDP) PI Service Threshold: “Inadequate” (as defined in the SVDP) shall be considered below threshold	Yes
SPI-02	Proposal Turnaround	See Paragraph 9 of Part B of this Annex 1	Monthly	Target Performance Level: Zero Working Days beyond the deadline PI Service Threshold: Two or more Working Days beyond the deadline	Yes
SPI-03	Not Used				
SPI-04	Capacity Management	See Paragraph 8 of Part B of this Annex 1	Monthly	Target Performance Level: 99% PI Service Threshold 96%	No

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Performance levels	Publishable Performance Information
SPI-05	CMDB Accuracy	See Paragraph 11 of Part B of this Annex 1	Quarterly	Target Performance Level: 99.6% PI Service Threshold: Below 98%	No
SPI-06	Root Cause Analysis Reporting	See Paragraph 12 of Part B of this Annex 1	Monthly	Target Performance Level: 100%, where there are 100 or more Root Cause Analysis reports in a Service Period; or - Zero late Root Cause Analysis reports where there are fewer than 100 Root Cause Analysis reports in a Service Period. PI Service Threshold: - Below 93%, where there are 100 or more Root Cause Analysis reports in a Service Period; or - Seven or more late Root Cause Analysis reports where there are fewer than 100 Root Cause Analysis reports in a Service Period.	Yes

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Performance levels	Publishable Performance Information
SPI-07	Aged Service Incident Management	See Paragraph 3.15 of Part B of this Annex 1	Monthly	Target Performance Level: 95% PI Service Threshold: Below 93%	Yes
SPI-08	Vulnerability Management	See Paragraph 13 of Part B of this Annex 1	Monthly	Target Performance Level: 0 days' overdue PI Service Threshold: Critical patches: 7 days' overdue Other patches: 15 days' overdue	No
SPI-09	Core Network Services Availability	See Paragraph 2.1 of Part B of this Annex 1	Monthly	Target Performance Level: 99.9% PI Service Threshold: Below 98%	Yes

OPTIONAL SERVICES

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

3 Performance Indicators for Optional Services

- 3.1 Following commencement of any Optional Services in accordance with Clause 5.12, all relevant Performance Indicators set out in Paragraphs 1, 2 and 3.5 of this Part A of Annex 1 shall apply to the relevant Optional Services from the third Service Period following commencement of the Optional Service (unless otherwise agreed in the Optional Services Implementation Plan).
- 3.2 Not used.
- 3.3 Where the Supplier acts as a reseller to the Authority of service subscriptions, the Supplier shall ensure that all service levels and rights and remedies available under the relevant service subscription shall be available to the Authority.
- 3.4 Notwithstanding Paragraph 1.1 of this Schedule 3 (*Performance Levels*), “**Resolution**” in relation to a SASE Service Incident shall mean a field engineer has physically checked the SD-WAN Edge Device and has followed the Incident Management Process to the satisfaction of the Authority to either (1) repair the cause(s) of the Service Incident or (2) implement a Workaround or (3) inform the Authority on what other actions will be necessary to address the SASE Service Incident; and “Resolved” shall be construed accordingly for SASE Service Incidents.
- 3.5 The Key Performance Indicator(s) in Table 2 set out in Paragraph 1.1 above shall apply to the relevant Optional Services.

Table 4 –Not used

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Part B: Definitions

1 AVAILABLE

- 1.1 The IT Environment and/or the Services shall be Available when:
- (a) End Users are able to access and utilise all the functions of the IT Environment and/or the Services; and
 - (b) the IT Environment and/or Services are able to process data and to provide any required reports within the timescales set out in the Authority Requirements; and
 - (c) in respect of Core Network Services only, the Vulnerability Management Performance Indicator for the Gateway Test System is above the PI Service Threshold; and
 - (d) in respect of the Gateway System only, the Vulnerability Management Performance Indicator for the Gateway System (excluding the Gateway Test System) is above the KPI Service Threshold.

2 AVAILABILITY

- 2.1 For the purposes of this Annex 1, the following expressions shall have the meanings set opposite them below:
- | | |
|--|--|
| “Availability: Core Network Services” | Availability measured for each of the following Core Network Services: NTP, Gateway Test System and DNS Interfacing |
| “Availability: Gateway System” | Availability of the Gateway System excluding the Gateway Test System. |
| “Availability-Monitored Services” | The Services in scope of the Availability Performance Indicators. |
| “Availability Performance Indicator” | A Performance Indicator which measures the time that Services are Available, being: <ul style="list-style-type: none">(a) Availability: WAN Connectivity;(b) Availability: Gateway System; and(c) Availability: Core Network Services. |
| “Availability: WAN Connectivity” | Availability measured at each Authority Site of WAN Connectivity. |
- 2.2 **“Availability”** shall be measured for each Availability Performance Indicator as the percentage of the total time in a Service Period that the relevant

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Availability-Monitored Services are Available, in accordance with the following formula:

$$\text{Availability \%} = \frac{(MP - SD) \times 100}{MP}$$

where:

MP = total number of minutes, excluding Permitted Maintenance, within the relevant Service Period; and

SD = total number of minutes of Service Downtime, excluding Permitted Maintenance, in the relevant Service Period.

2.3 When calculating Availability in accordance with this Paragraph 2:

- (a) Service Downtime arising due to Permitted Maintenance that is carried out by the Supplier in accordance with Clause 9.4 (*Maintenance*) shall be subtracted from the total number of hours in the relevant Service Period; and
- (b) Service Points shall accrue if:
 - (i) any Service Downtime occurs as a result of Emergency Maintenance undertaken by the Supplier; or
 - (ii) where Service Downtime for Permitted Maintenance undertaken by the Supplier exceeds the period booked in accordance with Paragraph 4.1 of Part A of this Schedule, in any Service Period.

2.4 “Availability: WAN Connectivity” performance levels for each classification of Authority Site are shown in Table 5 below.

Table 5 – Availability: WAN Connectivity performance levels

Performance Level	Each Gold Site	Each Silver Site	Each Bronze Site
Target Performance Level	99.99%	99.95%	99.9%
Minor KPI Failure	99.7% – 99.98%	99.5% – 99.94%	99.5% – 99.89%
Serious KPI Failure	99.5% – 99.69%	99% – 99.49%	99% – 99.49%
Severe KPI Failure	99% – 99.49%	98% – 98.99%	98% – 98.99%
KPI Service Threshold	Below 99%	Below 98%	Below 98%

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 2.5 In respect of “Availability: WAN Connectivity”, if a KPI Failure occurs at any two or more separate Authority Sites during a Service Period the second and any subsequent such KPI Failure shall be recorded as a separate KPI Failure and the relevant Service Points shall apply to each KPI Failure.
- 2.6 In respect of “Availability: Core Network Services”, if a Performance Failure occurs in respect of any two or more L3 Core Network Services during a Service Period, the second and any subsequent such Performance Failure shall be recorded as a separate Performance Failure.
- 2.7 Not used.
- 2.8 If any Availability Performance Indicator(s) cannot be measured in accordance with this Schedule 3 (*Performance Levels*) owing to impaired function of the Supplier System:
- (a) the Supplier may provide measurement data and analysis in other ways, and the Authority shall decide, acting reasonably, to what extent (if any) it will take such data and measurement into account in respect of the relevant Availability Performance Indicator(s);
 - (b) the Authority shall seek to infer Availability status from data sources available, including information provided by the Supplier in accordance with Sub-paragraph 2.8(a) and ITSM Toolset records (e.g. Service Incident logs); and
 - (c) if Availability cannot be ascertained or inferred in accordance with Sub-paragraphs 2.8(a) and 2.8(b), the Performance Level achieved for the relevant Authority Site or In-Scope Services shall be a Serious KPI Failure.

3 INCIDENT RESOLUTION TIMES

- 3.1 Resolution Times for Severity 1 Service Incidents and Severity 2 Service Incidents shall be measured 24x7, excluding On Hold Time.
- 3.2 Resolution Times for Severity 3 Service Incidents and Severity 4 Service Incidents shall be measured in Service Hours, excluding On Hold Time.

Worked example: if the Service Hours for a fault are 08:00 – 21:30, then the clock stops measuring Resolution Time at 21:30 in the evening and restarts at 0800 the following day.

- 3.3 The priority of a Service Incident will be assigned by the Authority based on the Authority’s assessment of the Service Incident’s impact and urgency in accordance with the Authority’s incident management process, using the severity levels defined in Table 6:

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Table 6 – Service Incident severity levels

Service Incident severity	Title (for information used in Authority's incident management process.)	Description
1	Major incident	Failure, or Unavailability, or reduction in performance or loss of functionality of all or part of the Services that prevents a group of End Users from completing their work resulting in critical business impact where there is no alternative way to work. For example: - Connectivity is lost to a resilient Authority Site resulting in critical business impact; Access to ViSOR is lost; - Business applications critical to delivery of the Authority's and/or Service Recipients' services cannot be used.
2	High	Failure, or Unavailability, or reduction in performance or loss of functionality of all or part of the Services that results in significant business impact where there is no alternative way to work. For example: - An Authority Site is unable to access email services due to a routing issue in the Supplier's network; or - Loss of key Supplier ITSM capability, for example, loss of monitoring capability.
3	Medium	Failure, or Unavailability, or reduction in performance or loss of functionality of all or part of the Services without significant business impact; Or A single End User is impacted by Unavailability, loss of functionality or a reduction in performance of all or part of the Services. For example:

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

		• Resilience is lost at a resilient Authority Site; or • Loss of the Gateway Test System.
4	Low	Any other Service Incident that is none of the above and has no impact from an End User perspective but requires management.

And the expressions “**Severity 1 Service Incident**”, “**Severity 2 Service Incident**”, *etc.* shall be interpreted with reference to the Service Incident severities in Table 6.

- 3.3A Notwithstanding the priority assigned under the Authority’s incident management process in accordance with Paragraph 3.3, all Service Incidents which affect only Bronze Sites shall be measured as Severity 3 Service Incidents for the purposes of this Schedule 3.
- 3.4 Examples given in Table 6 are non-exhaustive and for general guidance only, as they may not reflect all circumstances which may arise in connection with a Service Incident. For example, there may be circumstances where a Service Incident affecting a single End User has a significant business impact. To note, the Severity of a Service Incident can be changed at any time by the Authority as described in the Processes.
- 3.5 The Authority may by giving notice to the Supplier in writing from time to time within the Authority Site List:
- designate an Authority Site that is vital to the delivery of the Authority’s and/or Service Recipient’s mission-critical activities as a “**VIP Site**”; and
 - de-classify an Authority Site so that it is no longer designated as a VIP Site,
- provided that the total number of VIP Sites at any time does not [REDACTED] Authority Sites.
- 3.6 Notwithstanding Paragraph 3.3, the Authority may require the Supplier to apply a higher priority to, or to use best endeavours to achieve urgent Resolution of, any Service Incident relating to a VIP Site, and the Supplier shall comply with this requirement.
- 3.7 For the avoidance of doubt, Paragraph 3.6 shall not affect the Service Incident severity level for the purposes of measuring the Key Performance Indicators.
- 3.8 The Authority may by giving notice to the Supplier in writing from time to time amend the Site Type for an Authority Site, subject to compliance with the definitions of Bronze Site, Silver Site, Gold Site respectively in accordance

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

with Schedule 1 (Definitions), provided that the total number of amendments to Site Types does not exceed ten (10) in any rolling twelve-month period.

3.9 Not used.

3.10 The Resolution Deadlines shall be a Resolution Time of:

- for Severity 1 Service Incidents, two (2) hours;
- for Severity 2 Service Incidents, four (4) hours;
- for Severity 3 Service Incidents, eight (8) Service Hours; and
- for Severity 4 Service Incidents, three (3) Working Days.

3.11 “**Incident Resolution Time**” shall be measured as follows:

(a) for Severity 1 Service Incidents and Severity 2 Service Incidents, per Service Incident open at any time during the relevant Service Period, as the number of minutes’ Resolution Time greater than the Resolution Deadline;

(b) for Severity 3 Service Incidents:

(i) where the number of Severity 3 Service Incidents open at any time during the relevant Service Period is 100 or more, according to the following formula:

$$\text{Incident Resolution Time \%} = \frac{(SI - UI) \times 100}{SI}$$

where:

SI = total number of Severity 3 Service Incidents open at any time during the relevant Service Period; and

UI = total number of Severity 3 Service Incidents open at any time during the relevant Service Period where the Resolution Time is greater than eight (8) Service Hours; and

(ii) where the number of Severity 3 Service Incidents open at any time during the relevant Service Period is fewer than 100, the number of Severity 3 Service Incidents open at any time during the relevant Service Period where the Resolution Time is greater than the Resolution Deadline, (“**Late Severity 3 Service Incidents**”).

3.12 Performance levels for Incident Resolution Time of Severity 1, Severity 2 and Severity 3 Service Incidents shall be measured in relation to how late the Resolution Time is against the required Resolution Deadline in accordance with Paragraph 3.10, as shown in Table 7:

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Table 7 – Performance levels for Incident resolution Time: Severity 1, 2 and 3 Service Incidents

Performance level	Severity 1 Service Incidents	Severity 2 Service Incidents	Severity 3 Service Incidents	
			<100 Severity 3 Service Incidents in a Service Period	>99 Severity 3 Service Incidents in a Service Period
Target Performance Level	0 minutes late	0 minutes late	Up to one Late Severity 3 Service Incident	98%
Minor KPI Failure	>1 minute late; up to 2 hours late	>1 minute late; up to 2 hours late	Two Late Severity 3 Service Incidents	97.51% – 97.99%
Serious KPI Failure	>2 hours late; up to 4 hours late	>2 hours late; up to 8 hours late	Three Late Severity 3 Service Incidents	97.01% – 97.5%
Severe KPI Failure	>4 hours late; up to 10 hours late	>8 hours late; up to 20 hours late	Four Late Severity 3 Service Incidents	96.01% – 97%
KPI Service Threshold	>10 hours late	>20 hours late	Five or more Late Severity 3 Service Incidents	Below 96.01%

3.13 Service Points (“**SP**”) for Incident Resolution Time of Severity 1, Severity 2 and Severity 3 Service Incidents shall:

- (a) be incurred if the Resolution Time has a performance level of Minor KPI Failure, Serious KPI Failure or Severe KPI Failure as shown in Table 7; and
- (b) be calculated as a fixed number of Service Points plus additional Service Points at a rate of one additional Service Point per interval of time, depending on the applicable performance level in accordance with Table 8.

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Table 8 – Service Points for Incident Resolution Time: Severity 1, 2 and 3

Performance level	Severity 1 Service Incidents	Severity 2 Service Incidents	Severity 3 Service Incidents
Target Performance Level	0 SP	0 SP	0 SP
Minor KPI Failure	22 SP; then 1 additional SP per 5 minutes	20 SP; then 1 additional SP per 6 minutes	10 SP
Serious KPI Failure	46 SP; then 1 additional SP per 4 minutes	40 SP; then 1 additional SP per 10 minutes	20 SP
Severe KPI Failure	76 SP; then 1 additional SP per 2 minutes	76 SP; then 1 additional SP per 5 minutes	30 SP
KPI Threshold	256 SP; then 1 additional SP per 2 minutes	256 SP; then 1 additional SP per 5 minutes	40 SP

3.14 For information only, the Service Points accrual in Paragraph 3.13 is illustrated in Annex H to Part E of Schedule 15 (Charges and Invoicing).

3.15 **“Service Incident Management”** shall be measured according to the following formula:

$$\text{Aged Service Incident Management \%} = \frac{(I - AI) \times 100}{I}$$

where:

I = total number of Service Incidents within the relevant Service Period; and

AI = total number of Aged Service Incidents within the relevant Service Period; and

“Aged Service Incident” means a Service Incident without Resolution after twenty (20) Working Days from the date it was reported to the Supplier.

4 SECURITY INCIDENT RESPONSE & RESOLUTION

4.1 For the purposes of this Paragraph 4, the following expressions shall have the meanings set opposite them below:

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“Response Deadline”	the deadline for Response in accordance with Paragraph 4.3
“Response Time”	the period from the time that the Security Incident is assigned to the Supplier to the time when the assigned Security Incident is accepted by the Supplier;
“Security Incident Management Process”	has the same meaning as “Incident Management Process” as defined in Schedule 5 (Security Management);
“Security Incident Resolution Plan”	a plan of actions is agreed with the Authority in accordance with the Security Incident Management Process to investigate, diagnose, resolve, and prevent future occurrences of the Security Incident;
“Severity 1 Security Incident”	a Security Incident which, in the reasonable opinion of the Authority: (a) causes, or may cause, the degradation of vital services for a large number of End Users and involves a serious breach of network security and/or affects mission-critical equipment or services and/or damages public confidence in the Government; (b) is, or is suspected to be, a concerted, repeating, targeted, effort causing harm to confidentiality, integrity or availability of ICT systems or data; or (c) causes, or may cause, loss of an information-bearing asset where it has not been verified that the data is in a secure state.
“Severity 2 Security Incident”	a Security Incident which, in the reasonable opinion of the Authority: (a) impacts, or may impact, a smaller group of End Users than a Severity 1 Service Incident and disrupts non-essential services and/or breaches network security policy and/or affects the reputation of Government bodies and services; or

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) is, or is suspected to be, a targeted attack attempting to cause harm to confidentiality, integrity or availability of ICT systems or data.

“Severity 3 Security Incident”

a Security Incident which, in the reasonable opinion of the Authority:

- (a) does not typically impact IT services, such as unsuccessful denial-of-service attacks and the majority of network monitoring alerts; or
- (b) causes, or may cause, loss of an information-bearing asset where the data is in a secure state; or
- (c) instances where activity or behaviour is recognised as suspicious but lacks supporting evidence.

“Severity 4 Security Incident”

a Security Incident which, in the reasonable opinion of the Authority is part of normal IT support operations. Such Security Incidents include receipt of an isolated spam or anti-virus alert, minor computer hardware failure, loss of network connectivity to a peripheral device or loss of access to a third party, non-essential service.

4.2 For the avoidance of doubt, where a Security Incident is detected in relation to a Service Incident (as defined in Paragraph 1 (*Definitions*) of this Schedule 3), the Response Time and Resolution Time of that Security Incident shall not include the period of time prior to it being identified as a Security Incident.

4.3 The deadlines for Response Times shall be:

- for Severity 1 Security Incidents, thirty (30) minutes;
- for Severity 2 Security Incidents, one (1) hour;
- for Severity 3 Security Incidents, four (4) Service Hours;
- for Severity 4 Security Incidents, eight (8) Service Hours.

4.4 The Resolution Deadlines for Security Incidents shall be:

- (a) the required Resolution Time specified in the Security Incident Resolution Plan, where such Security Incident Resolution Plan is required in accordance with the Security Incident Management Process; or

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) if not specified in the Security Incident Resolution Plan:
- for Severity 1 Security Incidents, two (2) hours;
 - for Severity 2 Security Incidents, four (4) hours;
 - for Severity 3 Security Incidents, 28 (twenty-eight) Service Hours;
 - for Severity 4 Security Incidents, 56 (fifty-six) Service Hours; or
- (c) as otherwise agreed with the Authority.

4.5 **“Security Incident Response Time”** shall be measured per Security Incident open at any time during the relevant Service Period, as the number of minutes’ Response Time greater than the Response Deadline.

4.6 Performance levels for Security Incident Response Time shall be measured in relation to how late the Security Incident Resolution Time is against the required Response Deadlines for Response Times to Security Incidents in accordance with paragraph 4.3, as shown in Table 9.

Table 9 – Security Incident Response Time performance levels

Performance level	Severity 1 Security Incidents	Severity 2 Security Incidents	Severity 3 Security Incidents	Severity 4 Security Incidents
Target Performance Level	0 minutes late	0 minutes late	0 minutes late	≤1 Service Hour late
Minor KPI Failure	>1 minute late; up to 30 minutes late	>1 minute late; up to 1 hour late	>1 minute late; up to 4 Service Hours late	>1 Service Hour late
Serious KPI Failure	>30 minutes late; up to 2 hours late	>1 hour late; up to 4 hours late	>4 Service Hours late; up to 8 Service Hours late	N/A
Severe KPI Failure	>2 hours late; up to 3½ hours late	>4 hours late; up to 7 hours late	>8 Service Hours late;	N/A
KPI Service Threshold	>3½ hours late	>7 hours late	N/A	N/A

4.7 Service Points (“**SP**”) shall:

- (a) be incurred if the Security Incident Response Time has a performance level of Minor KPI Failure, Serious KPI Failure or

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Severe KPI Failure as shown in Table 9; and

- (b) be calculated as a fixed number of Service Points plus additional Service Points per interval of time, depending on the applicable performance level in accordance with Table 10.

Table 10 – Service Points accrual for Security Incident Response Time

Performance level	Severity 1 Security Incidents	Severity 2 Security Incidents	Severity 3 Security Incidents	Severity 4 Security Incidents
Target Performance Level	0 SP	0 SP	0 SP	0 SP
Minor KPI Failure	40 SP; then 4 SP per minute	30 SP; then 1 SP per minute	20 SP; then 1 SP per 6 minutes	0 SP
Serious KPI Failure	160 SP; then 4 SP per minute	90 SP; then 1 SP per minute	60 SP; then 1 SP per 6 minutes	0 SP
Severe KPI Failure	520 SP; then 4 SP per minute	310 SP; then 2 SP per minute	100 SP; then 1 SP per 6 minutes	0 SP
KPI Service Threshold	880 SP; then 4 SP per minute	630 SP; then 2 SP per minute	N/A	0 SP

- 4.8 “**Security Incident Resolution Time**” shall be measured per Security Incident open at any time during the relevant Service Period, as the number of minutes’ Resolution Time greater than the Response Deadline, excluding On Hold Time.
- 4.9 Performance levels for Security Incident Resolution Time shall be the number of minutes or hours greater than the Resolution Deadline, as shown in Table 11, unless otherwise agreed by the Authority in respect of a Security Incident Resolution Plan.

Table 11 – Security Incident Resolution Time performance levels

Performance level	Severity 1 Security Incidents	Severity 2 Security Incidents	Severity 3 Security Incidents
Target Performance Level	0 minutes late	0 minutes late	8 hours late

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Performance level	Severity 1 Security Incidents	Severity 2 Security Incidents	Severity 3 Security Incidents
Minor KPI Failure	>1 minute late; up to 2 hours late	>1 minute late; up to 4 hours late	>8 hours up to 2 Working Days late
Serious KPI Failure	>2 hours late; up to 6 hours late	>4 hours late; up to 12 hours late	≥ 2 Working Days late up to 3 Working Days late
Severe KPI Failure	>6 hours late; up to 12 hours late	>12 hours late; up to 24 hours late	≥3 Working Days late up to 4 working days late
KPI Service Threshold	>12 hours late	>24 hours late	≥4 Working Days late

- 4.10 Service Points (“SP”) for Security Incident Resolution Time shall accrue per Security Incident (i) at the moment that the Resolution Time is within the duration for the respective performance level (as shown in Table 11) and (ii) at a rate of Service Points per minute indicated in Table 12, while Resolution Time is within the duration for the respective performance level (as shown in Table 11).

Table 12 – Service Points accrual for Security Incident Resolution Time

Performance level	Severity 1 Security Incidents	Severity 2 Security Incidents	Severity 3 Security Incidents
Target Performance Level	0 SP	0 SP	0 SP
Minor KPI Failure	20 SP; then 1 SP per 5 minutes	10 SP; then 1 SP per 6 minutes	10 SP; then 5 SP per Service Hour
Serious KPI Failure	44 SP; then 1 SP per 4 minutes	50 SP; then 1 SP per 6 minutes	50 SP; then 10 SP per Service Hour
Severe KPI Failure	105 SP; then 1 SP per 3 minutes	130 SP; 1 SP per 6 minutes	130 SP; then 15 SP per Service Hour

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Performance level	Severity 1 Security Incidents	Severity 2 Security Incidents	Severity 3 Security Incidents
KPI Threshold	240 SP; then 1 SP per 3 minutes	250 SP; then 1 SP per 6 minutes	250 SP; then 15 SP per Service Hour

4.11 For information only, the Service Points accrual in Table 12 is illustrated in Annex H of Part E to Schedule 15 (Charges and Invoicing).

5 SERVICE MANAGEMENT CHANGES

5.1 For the purposes of this Paragraph 5, the following expressions shall have the meanings set opposite them below:

“Failed Change” a Service Change completed in the Service Period which is recorded as a cause and/or contributing factor of any Severity 1 Service Incident, Severity 2 Service Incident or Severity 3 Service Incident; and

“Change Management” shall be measured as follows:

- (a) where there are fewer than 100 Service Changes within the relevant Service Period – as the number of Failed Changes; or
- (b) where there are 100 or more Service Changes within the relevant Service Period – in accordance with the following formula:

$$\text{Change Management \%} = \frac{(C-U) \times 100}{C}$$

where:

C = total number of Service Changes completed within the relevant Service Period; and

U = total number of Failed Changes within the relevant Service Period.

5.2 As part of its continuous service improvement responsibilities, the Supplier shall periodically review Service Changes recorded as a cause and/or contributing factor of a Severity 4 Service Incident.

5.3 For the Change Management KPI (KPI-06), the Performance Levels are stated in Table 13 below.

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Table 13: Performance Levels for the Change Management KPI.

Volume in a Service Period	Target Performance Level	Minor KPI Failure	Serious KPI Failure	Severe KPI Failure	KPI Service Threshold
<100 Service Changes	Up to one Failed Change	Two Failed Changes	Three Failed Changes	Four Failed Changes	Five or more Failed Changes
>99 Service Changes	98%	97% – 97.99%	96.01% – 96.99%	95.01% – 96%	Below 95.01%

5.4 For a failure to achieve the Change Management KPI Service Threshold, 40 Service Points will be allocated and:

- (a) where there are fewer than 100 Service Changes within the relevant Service Period, 10 additional Service Points for each additional Failed Change above the KPI Service Threshold; and
- (b) where there are 100 or more Service Changes within the relevant Service Period, 10 additional Service Points for each percentage point below the KPI Service Threshold.

5.5 Not Used

6 SERVICE REQUEST FULFILMENT

6.1 “**Service Request Fulfilment**” shall be measured as Catalogue Item(s) fulfilled by the Supplier within the applicable lead time in accordance with Paragraph 3.5 of Part B of Schedule 22 (*Change Control Procedure, Service Requests & Projects*) as follows:

- (a) where fewer than 100 Catalogue Items were due during the relevant Service Period: as the number of Catalogue Items which were not fulfilled within the applicable lead time (“**Late Catalogue Items**”); or
- (b) where 100 or more Catalogue Items were due during the relevant Service Period: in accordance with the following formula:

$$\text{Service Request Fulfilment \%} = \frac{(S-U) \times 100}{S}$$

where:

S = total number of Catalogue Items due within the relevant Service Period; and

U = total number of Late Catalogue Items within the relevant Service Period.

6.2 The measurement of time taken to fulfil Catalogue Item(s) shall exclude On Hold Time.

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

6.3 For the Service Request Fulfilment KPI (KPI-07), the Performance Levels are stated in Table 14 below.

Table 14: Performance Levels for the Service Request Fulfilment KPI

Volume in a Service Period	Target Performance Level	Minor KPI Failure	Serious KPI Failure	Severe KPI Failure	KPI Service Threshold
<100 Catalogue Items	Up to one Late Catalogue Item	Two Late Catalogue Items	Three Late Catalogue Items	Four Late Catalogue Items	Five or more Late Catalogue Items
>99 Catalogue Items	98%	97% – 97.99%	96.01% – 96.99%	95.01% – 96%	Below 95.01%

6.4 For a failure to achieve the Service Request Fulfilment KPI Service Threshold, 40 Service Points will be allocated and:

- (a) where fewer than 100 Catalogue Items were due to be achieved during the relevant Service Period, 10 additional Service Points for each additional Late Catalogue Item above the KPI Service Threshold; and
- (b) where 100 Catalogue Items or more were due to be achieved during the relevant Service Period, 10 additional Service Points for each percentage point below the KPI Service Threshold.

7 KNOWLEDGE MANAGEMENT

7.1 For the purposes of this Paragraph 7 the following expressions shall have the meanings set opposite them below:

- “Current Record”** subject to Paragraph 7.6 of Part B of this Annex 1, a Record which is complete and which the Supplier has, within 20 Working Days of the relevant Record Update Due Date, reviewed and confirmed as being accurate and up to date in respect of the Services;
- “Record Update Due Date”** the date by which a Record is due to be updated in accordance with the ‘update requirement’ column of the Table located in Annex 3 (*Records to Upload To Virtual Library*) of Schedule 24 (*Reports and Records Provisions*) or as otherwise agreed by the Authority; and
- “Knowledge Management Artefact”** Records indicated as in scope of this "Knowledge Management" Performance Indicator in the ‘in scope of knowledge management KPI’ column in Annex 3

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

(Records to Upload To Virtual Library) of Schedule 24
(Reports and Records Provisions).

7.2 “Knowledge Management” shall measure the completeness of the Knowledge Management Artefacts as follows:

- (a) where there are fewer than 100 Knowledge Management Artefacts due to be created or updated within the relevant Service Period – as the number of Knowledge Management Artefacts that are missing and/or not Current Records at the end of the Service Period (“Late Knowledge Management Artefacts”);
- (b) where there are 100 or more Knowledge Management Artefacts due to be created or updated within the relevant Service Period, according to the following formula:

Knowledge Management % = $\frac{(K-D) \times 100}{K}$

where:

- K = total number of Knowledge Management Artefacts due to be created or updated during the relevant Service Period, subject to Paragraph 7.5 of Part B of this Annex 1; and
- D = total number of Knowledge Management Artefacts due to be created or updated within the relevant Service Period which are missing and/or not Current Records at the end of the Service Period.

7.3 For the Knowledge Management KPI (KPI-08), the Performance Levels are stated in Table 14 below.

Table 15: Performance Levels for the Knowledge Management KPI

Volume in a Service Period	Target Performance Level	Minor KPI Failure	Serious KPI Failure	Severe KPI Failure	KPI Service Threshold
<100 Knowledge Management Artefacts	Up to one Late Knowledge Management Artefact	Two Late Knowledge Management Artefacts	Three Late Knowledge Management Artefacts	Four Late Knowledge Management Artefacts	Five or more Late Knowledge Management Artefacts
>99 Knowledge Management Artefacts	98%	97% – 97.99%	96.01% – 96.99%	95.01% – 96%	Below 95.01%

7.4 For a failure to achieve the Knowledge Management KPI Service Threshold, 40 Service Points will be allocated and:

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (a) where fewer than 100 Knowledge Management Artefacts are due to be created or updated during the relevant Service Period, 10 additional Service Points will be allocated for each additional Late Knowledge Management Artefact above the KPI Service Threshold; and
 - (b) where 100 or more Knowledge Management Artefacts are due to be created or updated during the relevant Service Period, 10 additional Service Points will be allocated for each percentage point below the KPI Service Threshold.
- 7.5 Where the Supplier has been relieved of responsibility to maintain any Records, in accordance with Paragraph 4.18 of Schedule 24 (*Reports and Records Provisions*), such Records shall be excluded from the number of Knowledge Management Artefacts calculated for parameters *K* and *D* in the formula in Paragraph 7.2(b).
- 7.6 Notwithstanding the definition of Current Record in Paragraph 7.1, Records that the Authority considers (acting reasonably) are inaccurate, incomplete or out-of-date shall not be considered to be Current Records until the Supplier has completed the required relevant amendments as notified by the Authority.

8 CAPACITY MANAGEMENT

- 8.1 “**Capacity Management**” shall be measured as the percentage of Resolved Service Incidents in a Service Period without a capacity-related Resolution code as recorded in the ITSM Toolset.
- 8.2 When calculating Capacity Management in accordance with Paragraph 8.1, the following Service Incidents shall be excluded:
- (a) where the cause relates to capacity risk previously logged by the Supplier with mitigating action identified in the log as the Authority’s action and a reasonable timescale to complete such action, and where the Authority has not completed such action within the specified timescale, and where no Workaround is available; and
 - (b) where there is a non-typical surge in End User demand that exceeds 110% of the baseline demand.

9 PROPOSAL TURNAROUND

- 9.1 “**Proposal Turnaround**” shall be measured for each Project Proposal due within the Service Period in accordance with Paragraph 5.1 (*Project Proposals*) of Part B of Schedule 22 (*Change Control Procedure, Service Requests & Projects*), including any Project Proposals overdue from previous Service Periods.
- 9.2 The measurement of “Proposal Turnaround” shall be the number of Working Days that the Project Proposal is overdue.

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 9.3 Where a Project Request has been withdrawn by the Authority before a Project Proposal has been provided by the Supplier, the Project Proposal which would have been due for that Project Request shall be excluded from the measurement of Proposal Turnaround.
- 9.4 Where the Supplier has set out reasonable grounds for the Project Proposal to be delayed, and that delay has been agreed with the Authority.

10 [NOT USED]

11 CMDB ACCURACY

11.1 “**CMDB Accuracy**” shall measure the accuracy and completeness of the information held in the CMDB as follows:

- (a) Within fifteen (15) Working Days of the end of each Measurement Period, the Supplier shall select a sample of two hundred and fifty (250) Assets from Authority Site(s) and using mandatory fields nominated by the Authority and measure the accuracy and completeness of the information held within the CMDB for those Assets;
- (b) The Supplier shall not select the same sample of Assets to be measured in two consecutive Measurement Periods, and the Supplier must sample at least ten percent (10%) of the volume of the Supplier CMDB in each Contract Year, following the second Operational Service Commencement Date;
- (c) Within ten (10) Working Days of completing the check in accordance with Sub-Paragraphs (a) and (b), the Supplier shall provide a report to the Authority containing the results; and
- (d)
$$\text{CMDB Accuracy \%} = \frac{A \times 100}{(250 - E)}$$

where:

A is the number of audited Assets correctly recorded in the CMDB in the Measurement Period; and

E is the number of Assets excluded in accordance with Paragraph 11.2.

11.2 The following Assets shall be excluded from the sample of those audited:

- (a) where the Asset has been moved, added to, or changed by the Authority or an Other Supplier and the Authority has not advised the Supplier of such move, add or change; and
- (b) any relevant exceptions in accordance with the Service Asset and Configuration Management process.

SCHEDULE 3 (PERFORMANCE LEVELS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

12 ROOT CAUSE ANALYSIS REPORTING

- 12.1 “Root Cause Analysis” shall be measured for each Root Cause Analysis Report due within the Service Period in accordance with the Service Management Requirements (including requirement numbers 6.3.1.3 and 6.5.3.3) and relevant Processes, including any Root Cause Analysis Reports overdue from previous Service Periods.
- (a) Where the number of Root Cause Analysis reports in a Service Period is 100 or more – Root Cause Analysis Reports which were not provided, as a percentage of all Root Cause Analysis Reports which were completed within the Service Period; or
 - (b) Where the number of Root Cause Analysis reports in a Service Period is less than 100 – as the total number of Root Cause Analysis reports not provided within the Service Period.

Table 16: Performance Levels for the Root Cause Analysis KPI Performance Level

Volume in a Service Period	Target Performance Level	PI Service Threshold
<100 RCA	Zero Late RCA reports	Seven Late RCA reports
>99 RCA	100%	93%

- 12.2 The measurement of “Root Cause Analysis” shall be the number of Working Days that the Root Cause Analysis Report is overdue without prior agreement from the Authority.

13 VULNERABILITY MANAGEMENT

- 13.1 “Vulnerability Management” shall be measured as the number of days taken to apply security patches under Paragraph 8.3.3 of Schedule 5 (Security Management) and Paragraph 17.5 of the Baseline Security Requirements for:
- (a) the Gateway Test System, measured separately from
 - (b) the Gateway System (excluding the Gateway Test System).
- 13.2 Each failure to patch a Device shall be treated as a separate PI Failure except to the extent that such Devices are of the same model.

Example: Failure to patch any or all of the [REDACTED] Devices would constitute a single PI Failure. Failure to also patch any or all of the [REDACTED] Devices during the same Service Period would constitute an additional PI Failure.

- 13.3 [REDACTED]

SCHEDULE 4 (STANDARDS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 4

STANDARDS

SCHEDULE 4 (STANDARDS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Schedule 4 (*Standards*)**1 DEFINITIONS**

1.1 In this Schedule, the following definitions shall apply:

“Standards Hub”	the Government’s open and transparent standards adoption process as documented at http://standards.data.gov.uk/ ; and
“Suggested Challenge”	a submission to suggest the adoption of new or emergent standards in the format specified on Standards Hub.

2 GENERAL

- 2.1 Throughout the term of this Contract, the Parties shall monitor and notify each other of any new or emergent standards which could affect the Supplier’s provision, or the Authority’s receipt, of the Services. Any changes to the Standards, including the adoption of any such new or emergent standard, shall be agreed in accordance with the Change Control Procedure.
- 2.2 Where a new or emergent standard is to be developed or introduced by the Authority, the Supplier shall be responsible for ensuring that the potential impact on the Supplier’s provision, or the Authority’s receipt, of the Services is explained to the Authority (in a reasonable timeframe), prior to the implementation of the new or emergent standard.
- 2.3 Where Standards referenced conflict with each other or with Good Industry Practice, then the later Standard or best practice shall be adopted by the Supplier. Any such alteration to any Standard(s) shall require the prior written agreement of the Authority and shall be implemented within an agreed timescale.

3 TECHNOLOGY AND DIGITAL SERVICES PRACTICE

- 3.1 The Supplier shall (when designing, implementing and delivering the Services) adopt the applicable elements of HM Government’s Technology Code of Practice as documented at <https://www.gov.uk/service-manual/technology/code-of-practice.html>.

4 OPEN DATA STANDARDS & STANDARDS HUB

- 4.1 The Supplier shall comply to the extent within its control with UK Government’s Open Standards Principles as documented at <https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles>, as they relate to the specification of standards for software interoperability, data and document formats in the IT Environment.

SCHEDULE 4 (STANDARDS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 4.2 Without prejudice to the generality of Paragraph 2.2, the Supplier shall, when implementing or updating a technical component or part of the Software or Supplier Solution where there is a requirement under this Contract or opportunity to use a new or emergent standard, submit a Suggested Challenge compliant with the UK Government's Open Standards Principles (using the process detailed on Standards Hub and documented at <http://standards.data.gov.uk/>). Each Suggested Challenge submitted by the Supplier shall detail, subject to the security and confidentiality provisions in this Contract, an illustration of such requirement or opportunity within the IT Environment, Supplier Solution and Government's IT infrastructure and the suggested open standard.
- 4.3 The Supplier shall ensure that all documentation published on behalf of the Authority pursuant to this Contract is provided in a non-proprietary format (such as PDF or Open Document Format (ISO 26300 or equivalent)) as well as any native file format documentation in accordance with the obligation under Paragraph 4.1 to comply with the UK Government's Open Standards Principles, unless the Authority otherwise agrees in writing.

5 TECHNOLOGY ARCHITECTURE STANDARDS

- 5.1 The Supplier shall produce full and detailed technical architecture documentation for the Supplier Solution in accordance with Good Industry Practice. If documentation exists that complies with the Open Group Architecture Framework 9.2 or its equivalent, then this shall be deemed acceptable.

6 ACCESSIBLE DIGITAL STANDARDS

- 6.1 The Supplier shall comply with (or with equivalents to):
- (a) the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.1 Conformance Level AA;
 - (b) ISO/IEC 13066-1: 2011 Information Technology – Interoperability with assistive technology (AT) – Part 1: Requirements and recommendations for interoperability; and
 - (c) ISO/IEC 3071-1:2019 Information technology – Development of user interface accessibility.

7 SERVICE MANAGEMENT SOFTWARE & STANDARDS

- 7.1 Subject to Paragraphs 2 to 4 (inclusive), the Supplier shall reference relevant industry and HM Government standards and best practice guidelines in the management of the Services, including the following and/or their equivalents:
- (a) ITIL v3, as a minimum;
 - (b) ISO/IEC 20000-1 2018 "Information technology — Service management – Part 1";

SCHEDULE 4 (STANDARDS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (c) ISO/IEC 20000-2 2019 “Information technology — Service management – Part 2”;
- (d) ISO 10007: 2017 “Quality management systems – Guidelines for configuration management”; and
- (e) ISO 22313:2020 “Security and resilience. Business continuity management systems. Guidance on the use of ISO 22301” and, ISO/IEC 27031:2011 and ISO 22301:2019.

7.2 For the purposes of management of the Services and delivery performance the Supplier shall make use of Software that complies with Good Industry Practice including availability, change, incident, knowledge, problem, release & deployment, request fulfilment, service asset and configuration, service catalogue, service level and service portfolio management. If such Software has been assessed under the ITIL Software Scheme as being compliant to “Bronze Level”, then this shall be deemed acceptable.

8 SUSTAINABILITY

8.1 The Supplier shall comply with the sustainability requirements set out in the Annex 1 to this Schedule.

9 HARDWARE SAFETY STANDARDS

9.1 The Supplier shall comply with those BS or other standards relevant to the provision of the Services, including the following or their equivalents:

- (a) any new hardware required for the delivery of the Services (including printers), shall conform to BS EN IEC 62368-1:2020+A11:2020 or subsequent replacements. In considering where to site any such hardware, the Supplier shall consider the future working user environment and shall position the hardware sympathetically, wherever possible;
- (b) any new audio, video and similar electronic apparatus required for the delivery of the Services, shall conform to the following standard: BS EN IEC 62368-1:2020+A11:2020 or any subsequent replacements;
- (c) any new laser printers or scanners using lasers, required for the delivery of the Services, shall conform to either of the following safety Standards: BS EN 60825-1:2014 or any subsequent replacements; and
- (d) any new apparatus for connection to any telecommunication network, and required for the delivery of the Services, shall conform to the following safety Standard: BS EN 62949:2017 or any subsequent replacements.

SCHEDULE 4 (STANDARDS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 9.2 Where required to do so as part of the Services, the Supplier shall perform electrical safety checks in relation to all equipment supplied under this Contract in accordance with the relevant health and safety regulations.

10 Other Standards

- 10.1 The Supplier shall comply with and follow the policies and guidance listed in the table below, and as amended from time to time:

#	Standard
1	Cloud guide for the public sector as documented at: https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector
2	MoJ Cyber and Technical Security Guidance as documented at: https://security-guidance.service.justice.gov.uk
3	ISO/IEC 27001 – Information security, cybersecurity and privacy protection
4	ISO/IEC 27002 – Code of practice for information security management
5	ISO/IEC 27011 – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
6	ISO/IEC 27033 – Parts 1 to 4 Network security
7	HMG Functional Standard GovS 007: Security Government Functional Standard GovS 007: Security - GOV.UK (www.gov.uk);
8	NCSC Guidance as documented at: https://www.ncsc.gov.uk/section/advice-guidance/all-topics
9	NCSC Cyber Assessment Framework as documented at: https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework
10	MoJ ICT Physical Infrastructure Standards v4.2
11	MoJ Project Delivery Standards
12	Where the Supplier provides the Optional Service, PSN Access: PSN code of connection as documented at: https://www.gov.uk/government/publications/psn-code-of-connection-coco; and

SCHEDULE 4 (STANDARDS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	PSN Compliance v3.7, Jul 2012 and PSN Technical Domain Description V4.0.
13	Where applicable for the delivery of the Services, the HMPPS Prison Service Orders (PSO), Prison Service Instructions (PSI) and Prison and Probation Policy Frameworks which are available at: - Prison and Probation Policy Frameworks - GOV.UK (www.gov.uk) (https://www.gov.uk/government/collections/prison-probation-policy-frameworks) - Prison service instructions (PSIs) - GOV.UK (www.gov.uk) (https://www.gov.uk/guidance/prison-service-instructions-psis) - Prison service orders (PSOs) - GOV.UK (www.gov.uk) (https://www.gov.uk/guidance/prison-service-orders-psos).
14	Where applicable for the delivery of the Services, the relevant Criminal Justice System (CJS) Standards which are available at criminal justice system: data standards forum guidance (https://www.gov.uk/guidance/criminal-justice-system-data-standards-forum-guidance).

11 INCOME SECURITY**11.1 The Supplier shall:**

- (a) ensure that that all wages and benefits paid for a standard working week meet, at a minimum, national legal standards in the country of employment;
- (b) ensure that all Supplier Personnel are provided with written and understandable information about their employment conditions in respect to wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;
- (c) not make deductions from wages:
 - (i) as a disciplinary measure
 - (ii) except where permitted by law; or
 - (iii) without expressed permission of the worker concerned;
- (d) record all disciplinary measures taken against Supplier Personnel; and
- (e) ensure that Supplier Personnel are engaged under a recognised employment relationship established through national law and practice.

SCHEDULE 4 (STANDARDS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

12 WORKING HOURS

12.1 The Supplier shall:

- (a) ensure that the working hours of Supplier Personnel comply with national laws, and any collective agreements;
- (b) that the working hours of Supplier Personnel, excluding overtime, shall be defined by contract, and shall not exceed 48 hours per week unless the individual has agreed in writing;
- (c) ensure that use of overtime used responsibly, taking into account:
 - (i) the extent;
 - (ii) frequency; and
 - (iii) hours worked;by individuals and by the Supplier Personnel as a whole.

12.2 The total hours worked in any seven-day period shall not exceed 60 hours, except where covered by Paragraph 12.3 below.

12.3 Working hours may exceed 60 hours in any seven-day period only in exceptional circumstances where all of the following are met:

- (a) this is allowed by national law;
- (b) this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;
- (c) appropriate safeguards are taken to protect the workers' health and safety; and
- (d) the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.

12.4 All Supplier Personnel shall be provided with at least one (1) day off in every seven (7) day period or, where allowed by national law, two (2) days off in every fourteen (14) day period.

13 PROCESSES

13.1 The Supplier shall comply with and follow the Processes listed in the table below, and as amended from time to time:

No.	Process
1	Capacity Management

SCHEDULE 4 (STANDARDS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

No.	Process
2	Change and Evaluation Management
3	Continual Service Improvement
4	Demand Management
5	Event Management*
6	Incident Management
7	Knowledge Management
8	Licence Management and Compliance
9	Problem Management
10	Release and Deployment Management
11	Request Fulfilment
12	Service Asset and Configuration Management
13	Product and Service Catalogue Management
14	Service Level Management
15	Service Portfolio Management*
16	Transition Planning and Support
17	Availability Management
18	IT Service Continuity Management
19	Risk Management
20	Supplier Management
21	Service Desk
22	Technical Management

SCHEDULE 4 (STANDARDS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

No.	Process
23	Project Initiation
24	Major Incident Management
25	Transition Framework

**The Event Management and Service Portfolio Management Processes will be introduced by the Authority as new Processes after the Effective Date.*

- 13.2 Subject to Paragraph 13.3, if the Supplier believes that the introduction of and compliance with a new or revised Process will have a material and unavoidable effect on Costs, the Milestones, the Implementation Plan or Schedule 2 (Services Description) it may submit a Change Request. In doing so, the Supplier must support its request by providing evidence of the cause of any increased Costs or proposed Changes to the Milestones, the Implementation Plan or Schedule 2 (Services Description) and the steps that it has taken to mitigate those Costs or proposed Changes. Any Change to the Charges, the Milestones, the Implementation Plan or Schedule 2 (Services Description) shall then be agreed in accordance with the Change Control Procedure, but for the avoidance of doubt the Supplier shall not be entitled to increase its Charges to the extent that the Change in question would also be required under any other provision of this Contract and any increase in Charges shall also take account of any savings or non-incurrence of Costs as a result of the Change.
- 13.3 If the introduction of a new Process results from a Change in Law any effect on Costs arising out of the compliance with the new Process shall be borne by the Parties in accordance with the provisions of Clauses 13.2 to 13.4 inclusive (Change in Law).

SCHEDULE 4 (STANDARDS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 1: SUSTAINABILITY

1 DEFINITIONS

1.1 In this Annex 1, the following definitions shall apply:

“Permitted Item”	means those items which are permissible under this Contract to the extent set out in Table B of this Annex 1;
“Prohibited Items”	means those items which are not permissible under this Contract as set out at Table A of this Annex 1;
“Sustainability Reports”	written reports to be completed by the Supplier containing the information outlined in TABLE C of this Annex 1; and
“Waste Hierarchy”	means prioritisation of waste management in the following order of preference as set out in the Waste (England and Wales) Regulation 2011: (a) Prevention; (b) Preparing for re-use; (c) Recycling; (d) Other Recovery; and (e) Disposal.

2 PUBLIC SECTOR EQUALITY DUTY

2.1 In addition to legal obligations, where the Supplier is providing a Service to which the Public Sector Equality duty applies, the Supplier shall support the Authority in fulfilling its Public Sector Equality duty under S149 of the Equality Act 2010 by ensuring that it fulfils its obligations under the Contract in a way that seeks to:

- 2.1.1 eliminate discrimination, harassment or victimisation and any other conduct prohibited by the Equality Act 2010; and
- 2.1.2 advance:
 - (a) equality of opportunity; and
 - (b) good relations,

SCHEDULE 4 (STANDARDS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

between those with a protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership) and those who do not share it.

- 2.2 In delivering the Service, the Supplier will comply with the Authority's equality, diversity and inclusion requirements, to be provided to the Supplier by the Authority.
- 2.3 The Supplier shall ensure that it fulfils its obligations under the Contract in a way that does not discriminate against individuals because of socio-economic background, working pattern or having parental or other caring responsibilities.

3 ENVIRONMENTAL REQUIREMENTS

- 3.1 The Supplier must perform its obligations meeting in all material respects the requirements of all applicable Laws Contract regarding the environment.
- 3.2 The Supplier warrants that it has obtained relevant Environment Management System (EMS) certified to ISO 14001 or an equivalent certification from a UKAS accredited body and shall comply with and maintain certification requirements throughout the Term.
- 3.3 In performing its obligations under the Contract the Supplier shall, where applicable to the Contract, to the reasonable satisfaction of the Authority:
- (a) demonstrate low carbon resource efficiency, including minimising the use of resources and responding promptly to the Authority's reasonable questions;
 - (b) prioritise waste management in accordance with the Waste Hierarchy as set out in Law;
 - (c) be responsible for ensuring that any waste generated by the Supplier and sent for recycling, disposal or other recovery as a consequence of this Contract is taken by a licensed waste carrier to an authorised site for treatment or disposal and that the disposal or treatment of waste complies with the law;
 - (d) ensure that it and any third parties used to undertake recycling disposal or other recovery as a consequence of this Contract do so in a legally compliant way, and can demonstrate that reasonable checks are undertaken to ensure this on a regular basis and provide relevant data and evidence of recycling, recovery and disposal;
 - (e) in circumstances that a permit, licence or exemption to carry or send waste generated under this Contract is revoked, the Supplier shall cease to carry or send waste or allow waste to be carried by any Subcontractor until authorisation is obtained from the

SCHEDULE 4 (STANDARDS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Environment Agency; minimise the release of greenhouse gases (including carbon dioxide emissions), air pollutants, volatile organic compounds and other substances damaging to health and the environment;

- (f) reduce and minimise carbon emissions by taking into account factors including, but not limited to, the locations from which materials are sourced, the transport of materials, the locations from which the work force are recruited and emissions from offices and on-site equipment; and
 - (g) undertake the disposal of any electrical and electronic equipment in line with Waste Electrical and Electronic Equipment (WEEE) Regulations 2013.
- 3.4 In performing its obligations under the Contract, the Supplier shall to the reasonable satisfaction of the Authority (where the anticipated Charges in any Contract Year are above £5 million per annum (excluding VAT)), where related to and proportionate to the contract in accordance with PPN 06/21), publish and maintain a credible Carbon Reduction Plan in accordance with PPN 06/21.
- 3.5 The Supplier shall not provide to the Authority Goods or Deliverables which comprise wholly or partly of Prohibited Items unless such item is a Permitted Item.
- 3.6 The Supplier shall not use anything which comprises wholly or partly of the Prohibited Items to provide the Services under this Contract unless:
- (a) it is a Permitted Item; or
 - (b) the use is primarily related to the management of the Supplier's own facilities or internal operations as opposed to the provision of Services.
- 3.7 The Supplier must have a documented management system and controls in place to manage the environmental impacts of delivering the Services.
- 3.8 The Supplier shall ensure that any Services are designed, sourced and delivered in a manner which is environmentally and socially responsible.
- 3.9 In delivering the Services, the Supplier must comply with the Authority's sustainability requirements, to be provided to the Supplier by the Authority.
- 3.10 In performing its obligations under the Contract, the Supplier shall to the reasonable satisfaction of the Authority:
- 3.10.1 demonstrate that the whole life cycle impacts (including end of use) associated with the Services that extend beyond direct operations into that of the supply chain have been considered and reduced;

SCHEDULE 4 (STANDARDS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 3.10.2 minimise the consumption of resources and use them efficiently (including water and energy), working towards a circular economy including designing out waste and non-renewable resources, using re-use and closed loop systems;
 - 3.10.3 demonstrate protection of the environment including understanding and reduction of biosecurity risks (which include risks to plant and tree health from harmful pests and diseases), and reducing and eliminating hazardous/harmful substances to the environment and preventing pollution;
 - 3.10.4 enhance the natural environment and connecting communities with the environment; and
 - 3.10.5 achieve continuous improvement in environmental (and social) performance.
- 3.11 The Supplier shall inform the Authority within one Working Day in the event that a permit, licence or exemption to carry or send waste generated under this Contract is revoked.

ENVIRONMENTAL SUSTAINABILITY

- 3.12 The Supplier shall contribute towards the public sector's goal of improving the sustainability of ICT purchases and their operation via the Services supplied to under this Contract. I.e. such as recycling as much material from decommissioned racks as reasonably possible.
- 3.13 The Supplier shall, where required, support the Authority in developing their environmental policies, by providing advice on the best use of Services supplied and where appropriate by proposing innovative Services.
- 3.14 The Supplier is required to consider the impacts of their business processes on the environment and take measures to reduce such impact including by supporting where possible the Government's Environmental Policy and Sustainable Development Plan: <https://www.gov.uk/government/sustainable-development>.

ENERGY EFFICIENCY

- 3.15 The Supplier must consider the energy efficiency of all Goods and/or Services offered to the Authority and provide appropriate solutions and advice in accordance with:
- 3.15.1 DEFRA: Sustainability in information and communication technology (ICT): a Defra guide;

CARBON FOOTPRINT MEASUREMENT

- 3.16 The Suppliers shall provide Information on all relevant products and Services to assist Customers in the task of calculating their total carbon footprint.

SCHEDULE 4 (STANDARDS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 3.17 Suppliers must offer itemised carbon footprint figures for all Goods and/or Services.
- 3.18 External links for guidance:
 - 3.18.1 DEFRA: <https://uk-air.defra.gov.uk/>
 - 3.18.2 PAS2050: <http://shop.bsigroup.com/en/forms/PASs/PAS-2050>
 - 3.18.3 iSERVcmb: www.iSERVcmb.info

WASTE MANAGEMENT

- 3.19 In addition to the requirements in Paragraph 3.3, the Supplier shall ensure that they have adequate waste management solutions for the Services.
- 3.20 The Supplier shall where requested provide the Authority with a waste management strategy for the Services including refresh, refurbishment or reuse of equipment and environmental recovery, recycling or disposal options.
- 3.21 External links for guidance:
 - 3.21.1 WEEE Directive: <http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx> and <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0096:EN:NOT>
 - 3.21.2 RoHS Regulations: <https://www.gov.uk/guidance/rohs-compliance-and-guidance>

4 SUPPLIER ACCESSIBILITY RESPONSIBILITIES

- 4.1 Where required by the Authority, Suppliers shall provide suitable hardware and software to meet the diverse user needs. This may include individuals with a visual, auditory, physical, speech, cognitive, language, learning, behavioural or neurological impairment, as well as the needs of users for whom English is not their first language.
- 4.2 Suppliers shall assist the Authority in fulfilling their legal obligations with regards to accessibility, by offering help and guidance on how the Services can either support or be tailored to the Authority's needs.
- 4.3 Where required by the Authority, the Supplier shall provide an accessibility statement for Services provided under this Contract.
- 4.4 The Supplier shall where relevant maintain an accessibility policy, and identify (and where requested provide the details to the Authority) a role or department within their organisations with responsibility for the policy.

5 GOVERNMENT BUYING STANDARDS

- 5.1 The Supplier shall meet the applicable Government Buying Standards applicable to Services which can be found online at:

SCHEDULE 4 (STANDARDS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

<https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs>.

6 SUPPLIER CODE OF CONDUCT

- 6.1 In February 2019, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government which can be found online at:

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1163536/Supplier Code of Conduct v3.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1163536/Supplier_Code_of_Conduct_v3.pdf)

The Authority expects to meet, and expects its suppliers and subcontractors to meet, the standards set out in that Code.

7 REPORTING REQUIREMENTS

- 7.1 The Supplier shall comply with reasonable requests by the Authority for information evidencing compliance:

7.1.1 with Paragraphs 2.1, 3.1 to 3.6, 5.1 and 6 of this Annex 1 within fourteen (14) days of such request; and

7.1.2 With Paragraphs 2.2, 2.3 and 3.7 to 3.12 of this Annex 1 within thirty (30) days of such request,

provided that such requests are limited to two per Contract Year.

- 7.2 The Supplier shall complete the Sustainability Report in relation to its provision of the Services under this Contract and provide the Sustainability Report to the Authority on the date and frequency outlined in Table C of this Annex 1.

SCHEDULE 4 (STANDARDS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

TABLE A – PROHIBITED ITEMS

The following consumer single use plastics are Prohibited Items:	The prohibition on using these catering items is only intended to apply to Services delivered directly to the Authority. Catering a. Single use sachets e.g. coffee pods, sauce sachets, milk sachets b. Take away cutlery c. Take away boxes and plates d. Cups made wholly or partially of plastic e. Straws f. Stirrers g. Water bottles Facilities a. Single use containers e.g. hand soap, cleaning products b. Wipes containing plastic Office Supplies a. Plastic envelopes b. Plastic wrapping for brochures c. Paper or card which is bleached with chlorine Packaging a. Single use plastic packaging from deliveries where avoidable e.g. shrink wrapped packaging from office supplier or facilities products. b. Single use carrier bags
Authority specific Prohibitions	As per above Prohibited Items
Project specific Prohibitions	As may be specified by the Authority under a Project Request from time to time

SCHEDULE 4 (STANDARDS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

TABLE B - PERMITTED ITEMS

Authority Permitted Items	None identified as at the Effective Date
Project Specific Permitted Items	

TABLE C - SUSTAINABILITY REPORTS

Sustainability Report Name	Content of Report	Frequency of Report
Sustainability - General	as proportionate and relevant to the Contract, the key sustainability impacts identified; the sustainability improvements planned or delivered; and the risks to the Services of climate change, including mitigation, adaptation and continuity plans employed by the Supplier in response to those risks.	On the anniversary of the Effective Date
Waste created	By type of material the weight of waste categories by each means of disposal in the Waste Hierarchy with separate figures for disposal by incineration and landfill.	On or before the Effective Date and on the anniversary of the Effective Date.
Waste permits	Copies of relevant permits and exemptions for waste, handling, storage and disposal.	On or before the Effective Date, on the anniversary of the Effective Date and within ten (10) Working Days of there is any change or renewal to license or exemption to

SCHEDULE 4 (STANDARDS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

		carry, store or dispose waste
Greenhouse Gas Emissions	Detail the Scope 1 and Scope 2 GHG emissions associated with the delivery of the contract. Scope 3 emissions to be reported as required (Optional) Emissions reporting should be in accordance with established best practice and internationally accepted standards. Greenhouse gas reporting from emissions sources (Scope 1, Scope 2 and Scope 3), and specific activities as requested by the Authority. This may include activities such as transportation, energy use and waste disposal.	On the anniversary of the Effective Date
Water Use	Volume in metres cubed.	On the anniversary of the Effective Date

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 5

SECURITY MANAGEMENT

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

1. Definitions and Order of Precedence 3

2. Introduction.....7

3. Principles of Security 8

4. Core and Wider Information Management Systems 10

5. Security Management Plan 11

6. Security Assurance of the Core Information Management System 13

7. Certification Requirements 17

8. Security Testing.....19

9. Malicious Software 23

10. Breach of Security 23

11. Data Processing, Storage, Management and Destruction 25

12. Security Monitoring and Reporting 27

ANNEX 1: BASELINE SECURITY REQUIREMENTS 28

ANNEX 2: SECURITY REQUIREMENTS FOR SUB-CONTRACTORS 46

ANNEX 3: SECURITY MANAGEMENT PLAN TEMPLATE 50

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

1. Definitions and Order of Precedence**1.1 In this Schedule:**

“Anti-Malicious Software”	means software that scans for and identifies possible Malicious Software in the IT Environment;
“Authority Security Representative”	means the single point of contact, nominated by the Authority, who has overall responsibility for security in relation to this Contract;
“Baseline Security Requirements”	the Authority’s baseline security requirements, the current copy of which is contained in Annex 1 (Baseline Security Requirements), updated from time to time by the Authority and notified to the Supplier in accordance with Clauses 18.10 to 18.12 (inclusive);
“Breach of Security”	means the occurrence of: (a) any unauthorised access to or use of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System and/or any information or data (including the Confidential Information and the Authority Data) used by the Authority, the Supplier or any Sub-contractor in connection with this Contract; (b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including copies of such information or data, used by the Authority, the Supplier or any Sub-contractor in connection with this Contract; and/or (c) any part of the Supplier System ceasing to be compliant with the Certification Requirements, in each case as more particularly set out in the security requirements in Schedule 2 (Services Description) and the Baseline Security Requirements;
“Certification Requirements”	means the information security requirements set out in Paragraph 7;
“CHECK Service Provider”	means a company which has been certified by the National Cyber Security Centre, holds “Green Light” status and is authorised to provide the IT Health Check services required by Paragraph 8.1;

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

“CIMS Sub-contractor”	means a Sub-contractor that provides or operates the whole, or a substantial part, of the Core Information Management System;
“Core Information Management System”	means those information assets, IT systems and/or Sites which shall be subject to the Baseline Security Requirements in accordance with Paragraph 4.1 together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources);
“Cyber Essentials”	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;
“Cyber Essentials Plus”	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
“Cyber Essentials Scheme”	means the Cyber Essentials scheme operated by the National Cyber Security Centre;
“Gateway Device Software”	means the software (including firmware) installed on the Devices of the Gateway System;
“Higher Risk Sub-contractor”	means a Sub-contractor that Processes Authority Data, where that data includes either: (a) the Personal Data of 1000 or more individuals in aggregate during the period between the first Operational Service Commencement Date and the date on which this Contract terminates in accordance with Clause 4.1(b); or (b) any part of that data includes any of the following: (i) financial information (including any tax and/or welfare information) relating to any person; (ii) any information relating to actual or alleged criminal offences (including criminal records); (iii) any information relating to children and/or vulnerable persons; (iv) any information relating to social care;

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (v) any information relating to a person's current or past employment; or
- (vi) Special Category Personal Data; or
- (c) the Authority in its discretion, designates a Sub-contractor as a Higher Risk Sub-Contractor in any procurement document related to this Contract; or
- (d) the Authority considers in its discretion, that any actual or potential Processing carried out by the Sub-contractor is high risk;

"IT Health Check"

has the meaning given Paragraph 8.1.1;

"Medium Risk Sub-contractor"

means a Sub-contractor that Processes Authority Data, where that data

- (a) includes the Personal Data of between 100 and 10,000 individuals (inclusive) in the period between the first Operational Service Commencement Date and the date on which this Contract terminates in accordance with Clause 4.1(b); and
- (b) does not include Special Category Personal Data;

"Process"

means any operation which is performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

For the avoidance of doubt, this is the definition of "Process" that shall apply to this Schedule 5 (Security Management), and the definition of "Process" set out in Schedule 1 (Definitions) shall not apply to this Schedule 5 (Security Management);

"Remediation Action Plan"

has the meaning given in Paragraph 8.3.3(a);

"Required Changes Register"

means the register forming part of the Security Management Plan which records each of the changes that the Supplier has agreed with the Authority shall

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

	be made to the Core Information Management System and/or the Security Management Plan as a consequence of the occurrence of any of the events set out in Paragraph 6.14 together with the date on which each such change shall be implemented and the date on which each such change was implemented;
“Residual Risk Statement”	means the notice issued by the Authority under Paragraph 6.7;
“Risk Management Rejection Notice”	has the meaning given in Paragraph 6.7.2;
“Security Aspects Letter”	means a letter issued by the Authority and returned by the Supplier of Sub-contractor (as the case may be) with a signed declaration, in the format published by the Authority at: https://security-guidance.service.justice.gov.uk/security-aspect-letters/#security-aspects-letters ;
“Security Assurance”	means the assessment of the Services and the Core Information Management System in accordance with Paragraph 6 by the Authority or an independent information risk manager/professional appointed by the Authority;
“Security Assurance Decision”	means the decision of the Authority, taken in accordance with the process set out in Paragraph 6, to issue the Supplier with a Residual Risk Statement or a Risk Management Rejection Notice in respect of the Services and the Core Information Management System;
“Security Management Plan”	means the document prepared in accordance with the requirements of Paragraph 5 and in the format, and containing the information, specified in Annex 3 (<i>Security Management Plan Template</i>) ;
“Security Test”	has the meaning given Paragraph 8.1;
“Special Category Personal Data”	means the categories of Personal Data set out in article 9(1) and article 10 of the UK GDPR;
“Statement of Information Risk Appetite”	means the statement provided by the Authority under Paragraph 5.1 setting out the nature and level of risk that the Authority considers to be acceptable from the

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

operation of the Core Information Management System;

“Sub-contractor Security Requirements”

means those requirements set out in Annex 2; and

“Supplier Security Representative”

means the single point of contact, who shall be a member of the Key Personnel, nominated by the Supplier and approved by the Authority, who has overall responsibility for security in relation to this Contract;

“Wider Information Management System”

means those information assets, IT systems and/or Sites which will be used by the Supplier and/or its Sub-contractors to Process Authority Data and which do not form part of the Core Information Management System, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources).

1.2 If there is any conflict between:

1.2.1 this Schedule 5 (Security Management) and the Baseline Security Requirements, then this Schedule 5 shall prevail unless expressly stated otherwise in the Baseline Security Requirements; and

1.2.2 this Schedule 5 (Security Management) and the Security Aspects Letter, then (notwithstanding Sub-paragraphs 3.3.2 and 3.3.3), this Schedule 5 shall prevail.

2. Introduction

2.1 The Authority operates an integrated, through-life process in partnership with suppliers which is transparent, auditable, and consistently applied to safeguard the Authority's data and services. This process is scoped to provide security assurance across suppliers, supply chain, and both the Wider Information Management System and the Core Information Management System.

2.2 The Authority's security assurance approach is underpinned by NCSC Cyber Assessment Framework (CAF) and is aligned to the Authority's risk appetite. This provides Government organisations and their security functions with an effective mechanism to understand the level of cyber resilience and provide a common baseline level of resilience to achieve for new and existing services in line with:

2.2.1 the HMG and Authority Cyber Security Strategy which can be found at: <https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030>; and

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 2.2.2 the Authority's strategy which can be found at:
<https://www.gov.uk/government/publications/ministry-of-justice-cyber-security-strategy-2023-to-2028>

2.3 This Part A of this Schedule 5 sets out:

- 2.3.1 the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Contract to ensure the security of the Authority Data, the IT Environment, the Services and the Core and Wider Information Management Systems;
- 2.3.2 the process which shall apply to the Security Assurance of the Core Information Management System in Paragraph 6;
- 2.3.3 the Certification Requirements applicable to the Wider Information Management System in Paragraph 7;
- 2.3.4 the Security Tests which the Supplier shall conduct during the Term in Paragraph 8;
- 2.3.5 the Security Tests which the Authority may conduct during the Term in Paragraph 8.6;
- 2.3.6 the obligations on the Supplier to prevent the introduction of Malicious Software into the Wider Information Management System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Wider Information Management System in Paragraph 9; and
- 2.3.7 each Party's obligations in the event of an actual or attempted Breach of Security in Paragraph 10.

3. Principles of Security

- 3.1 The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Authority Data and, consequently on the security of:
- 3.1.1 the Sites;
- 3.1.2 the IT Environment;
- 3.1.3 the Core Information Management System; and
- 3.1.4 the Services.
- 3.2 Notwithstanding the involvement of the Authority in the Security Assurance of the Supplier, Sub-contractors, and both the Wider Information Management System and Core Information Management System, the Supplier shall be and shall remain responsible for:
- 3.2.1 the security, confidentiality, integrity and availability of the Authority Data whilst that Authority Data is under the control of the Supplier or

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

any of its Sub-contractors; and

3.2.2 the security of the Core and Wider Information Management Systems.

3.3 The Supplier shall:

3.3.1 comply with the Baseline Security Requirements;

3.3.2 sign and return the Security Aspects Letter to the Authority within five (5) Working Days of the Effective Date and comply with the policies and requirements set out therein (except that timings regarding the signing and return of the Security Aspects Letter shall apply and take precedence over timings set out in the template Security Aspects Letter);

3.3.3 ensure that all Sub-contractors that Process Authority Data:

(a) comply with the Sub-contractor Security Requirements; and

(b) unless the Processing to be undertaken by the relevant Sub-contractor is in scope of an Approved Security Management Plan, sign and return the Security Aspects Letter to the Authority in advance of any Processing and comply with the policies and requirements set out therein (except that timings regarding the signing and return of the Security Aspects Letter shall apply and take precedence over timings set out in the template Security Aspects Letter); and

3.3.4 ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Schedule, including any requirements imposed on Sub-contractors by Annex 2, from the first Operational Service Commencement Date and as required to Achieve the Milestones requiring security-related Deliverables as detailed in Schedule 13 (Implementation Plan).

3.4 "Security management" shall be included on the agenda of the relevant Board(s) (as determined by the Authority) in order to discuss and monitor security matters including:

3.4.1 the Security Assurance of the Core Information Management System; and

3.4.2 recommendations related to the Security Assurance of the Core Information Management System.

3.5 To facilitate the Supplier's design, implementation, operation, management and continual improvement of the Security Management Plan and the security of the Services and Core and Wider Information Management Systems and otherwise:

3.5.1 the Supplier shall provide access to the Supplier Personnel responsible for information assurance; and

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

3.5.2 the Authority shall provide access to its personnel responsible for information assurance,

in each case at reasonable times on reasonable notice.

3.6 The Authority shall appoint an Authority Security Representative and the Supplier shall appoint a Supplier Security Representative. The Authority Security Representative and the Supplier Security Representatives shall be appropriately qualified, competent and empowered to take action to safeguard the Authority Data.

3.7 The Supplier Security Representative shall:

3.7.1 be a suitably qualified individual with mission and resources to centrally manage, coordinate, develop, implement and maintain the cybersecurity and privacy controls;

3.7.2 ensure cybersecurity and privacy controls relevant to the Core and Wider Information Management Systems are in place, effective, and documented with appropriate context in the Security Management Plan; and,

3.7.3 ensure that mechanisms are in place at all times to review cybersecurity and privacy controls, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

3.8 The Authority Security Representative shall be the primary point of contact for the Supplier Security Representative.

4. Core and Wider Information Management Systems

4.1 The scope of the Core Information Management System shall be as stated in Paragraph 1.1 of the Baseline Security Requirements.

4.2 The Supplier shall produce a diagram documenting the components and systems forming part of, and the boundary between, the Core Information Management System and the Wider Information Management System. The diagram prepared under this Paragraph 4.2 shall form part of the Security Management Plan.

4.3 Any proposed change to the component parts of the Gateway System shall be managed in accordance with Paragraph 4.2 of the Technical Requirements.

4.4 Any proposed change to the scope of or the boundary between the Core Information Management System and the Wider Information Management System shall be subject to the Change Control Procedure.

4.5 The Supplier may not Process Authority Data unless and until the Supplier has:

4.5.1 signed and returned the Security Aspects Letter; and

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 4.5.2 provided confirmation satisfactory to the Authority that the Supplier System has completed an IT Health Check within the preceding 12 months.
- 4.6 The Supplier shall ensure that each Sub-contractor shall not Process Authority Data unless and until:
 - 4.6.1 the Sub-contractor's Processing is authorised under a Residual Risk Statement; or
 - 4.6.2 a Security Aspects Letter signed by the Sub-contractor has been provided to the Authority in accordance with Paragraph 3.3.3(b), and the Supplier has provided confirmation to the Authority's satisfaction that the relevant Sub-contractor element of the Supplier System has completed an IT Health Check within the preceding 12 months.
- 4.7 Prior to the issue of the Residual Risk Statement, the Supplier shall comply with any limitations specified by the Authority on Processing of Authority Data.
- 4.8 The Baseline Security Requirements in respect of the Core Information Management System are set out in Annex 1.

5. Security Management Plan*Preparation and purpose of the Security Management Plan*

- 5.1 The Authority may, at any time, provide the Supplier with a statement of information risk appetite (the "**Statement of Information Risk Appetite**").
- 5.2 The Supplier must document in the Security Management Plan how the Supplier and its Sub-contractors will:
 - 5.2.1 comply with the requirements (including the Baseline Security Requirements) set out in this Schedule 5 (*Security Management*) and the Contract in order to ensure the security of the Authority Data and the Core Information Management System; and
 - 5.2.2 ensure that the operation of the Core Information Management System and the provision of the Services does not give rise to any information security risks greater than those set out in that Statement of Information Risk Appetite (where one has been provided).
- 5.3 The Supplier must ensure that:
 - 5.3.1 the Security Management Plan accurately represents the Core Information Management System;
 - 5.3.2 the Core Information Management System will meet the requirements of this Schedule 5 (*Security Management*) and the Statement of Information Risk Appetite (where one has been provided); and
 - 5.3.3 the residual risks of the Core Information Management System are no greater than those provided for in the Statement of Information Risk

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Appetite (where one has been provided).

- 5.4 By the date specified in the Implementation Plan, the Supplier shall prepare and submit the Security Management Plan to the Authority.

Contents of the Security Management Plan

- 5.5 The Security Management Plan shall be structured in accordance with the template as set out in Annex 3 of this Schedule 5 and must include:

- 5.5.1 a formal risk assessment of, and a risk treatment plan for, the Core Information Management System;
- 5.5.2 the process for managing any security risks from Sub-contractors and third parties with access to the Services, the Core Information Management System or the Authority Data;
- 5.5.3 unless such requirement is waived by the Authority, the controls the Supplier will implement in respect of the Services and all processes associated with the delivery of the Services, including:
- (a) the Supplier System;
 - (b) the Sites; and
 - (c) the Authority System (to the extent that it is under the control of the Supplier); and
 - (d) any IT, Information and data (including the Confidential Information of the Authority and the Authority Data) to the extent used by the Authority or the Supplier:
 - (i) in connection with this Contract; or
 - (ii) in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;

- 5.5.4 the Required Changes Register;

- 5.5.5 evidence that the Supplier and each applicable Sub-contractor is compliant with:

- (a) the Certification Requirements;
- (b) the Baseline Security Requirements; and
- (c) the Security Requirements for Sub-contractors;

so far as those requirements apply;

- 5.5.6 the diagram documenting the Core Information Management System, the Wider Information Management System and the boundary between them (created under Paragraph 4.2);

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 5.5.7 an assessment of the Core Information Management System against the requirements of this Schedule 5 (*Security Management*), including the Baseline Security Requirements;
 - 5.5.8 the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Authority Data, the Authority, the Service Recipients, the Services and/or End Users; and
 - 5.5.9 details of the support the Supplier will provide to the Authority's security operations centre and protective monitoring functions, including the security logging and alerting information to be made available to the Authority and the method and interfaces for making such information available.
- 5.6 If as a result of an updated Statement of Information Risk Appetite provided by the Authority amendments are required to the Security Management Plan and such amendments may lead to the Supplier incurring additional costs, such costs shall be agreed under the Change Control Procedure.
- 6. Security Assurance of the Core Information Management System**
- 6.1 The Authority will undertake Security Assurance of the Core Information Management System in accordance with this Paragraph 6.
- 6.2 The Supplier acknowledges that the purpose of Security Assurance of the Core Information Management System is to ensure that:
- 6.2.1 the Security Management Plan accurately represents the Core Information Management System;
 - 6.2.2 the Authority has sufficient confidence that the Core Information Management System will meet the requirements of the Baseline Security Requirements and (where provided) the Statement of Information Risk Appetite;
 - 6.2.3 the security Deliverables delivered by the Supplier in relation to relevant Milestones are as required by Schedule 13 (Implementation Plan); and
 - 6.2.4 the residual risks of the Core Information Management System are acceptable to the Authority, being no greater than those provided for in the Statement of Information Risk Appetite (where provided).
- 6.3 The Security Assurance shall be performed by the Authority or by representatives appointed by the Authority.
- 6.4 In addition to any obligations imposed by Schedule 13 (Implementation Plan) or Schedule 14 (Testing Procedures) the Supplier must ensure that the Detailed Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Schedule 5, including any requirements imposed on Sub-contractors by Annex 2, from each relevant

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Operational Service Commencement Date.

6.5 In particular, the Detailed Implementation Plan must include:

6.5.1 the dates on which each subsequent iteration of the Security Management Plan will be delivered to the Authority for review and staged approval; and

6.5.2 the date by which the Supplier is required to have received a Residual Risk Statement from the Authority together with details of each:

- (a) tasks the Supplier must complete, including any required Security Tests;
- (b) Milestones which must be Achieved; and
- (c) Authority Responsibilities which must be completed

for the Supplier to receive a Residual Risk Statement pursuant to Paragraph 6.10.

6.6 To facilitate Security Assurance of the Core Information Management System, the Supplier shall provide the Authority and its authorised representatives with such information and/or documentation that the Authority or its authorised representatives may reasonably require.

6.7 The Authority shall, by the relevant date set out in the Implementation Plan, review the Security Management Plan and undertake such further investigations as it considers necessary or desirable and issue to the Supplier either:

6.7.1 a Residual Risk Statement which will then form part of the Security Management Plan, confirming that the Authority is satisfied that the identified risks to the Core Information Management System have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Authority; or

6.7.2 where the Authority considers that:

- (a) the identified risks to the Core Information Management System have not been adequately or appropriately addressed; or
- (b) the residual risks to the Core Information Management System have not been reduced:
 - (i) where the Authority has Provided a Statement of Information Risk Appetite, to the level anticipated by that statement; or
 - (ii) where the Authority has not Provided a Statement of Information Risk Appetite, to an acceptable level,

a rejection notice ("**Risk Management Rejection Notice**"), with the reasons for its decision.

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 6.8 If the Authority issues a Risk Management Rejection Notice, Paragraph 4.7 shall apply and within 20 Working Days of the date of the Risk Management Rejection Notice:
- 6.8.1 address all of the issues raised by the Authority in such notice;
 - 6.8.2 update the Security Management Plan, as appropriate; and
 - 6.8.3 notify the Authority that the Core Information Management System is ready for a Security Assurance Decision.
- 6.9 If the Authority issues a two or more Risk Management Rejection Notices during its review of a Security Management Plan in accordance with Paragraphs 6.7 and 6.8, the failure to receive a Residual Risk Statement shall constitute a material Default by the Supplier.
- 6.10 Subject to Paragraph 6.9, the process set out in Paragraphs 6.7 to 6.9 shall be repeated until such time as the Authority issues a Residual Risk Statement to the Supplier or terminates this Contract.
- 6.11 From the date that the Authority issues a Residual Risk Statement to the Supplier, the Security Aspects Letter shall no longer apply and shall be replaced by the Security Management Plan.
- 6.12 The Supplier shall not connect the Supplier System to the Core Information Management System before receiving a Residual Risk Statement unless otherwise agreed by the Authority in writing.

Monitoring and updating the Security Management Plan

- 6.13 The Supplier shall keep the Core Information Management System and Security Management Plan under review and shall update the Security Management Plan annually in accordance with this Paragraph and the Authority shall review the Security Assurance Decision annually and following the occurrence of any of the events set out in Paragraph 6.15.
- 6.14 The Supplier, where it plans to undertake, or after becoming aware of, any of the following:
- 6.14.1 a significant change to the components or architecture of the Core Information Management System;
 - 6.14.2 a significant change in the boundary between the Core Information Management System and the Wider Information Management System;
 - 6.14.3 a significant change in the operation of the Core Information Management System;
 - 6.14.4 the replacement of an existing, or the appointment of a new:
 - (a) CIMS Sub-contractor; or
 - (b) Sub-contractor that Processes Authority Data;

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

6.14.5 a significant change in the quantity of Personal Data held within the Wider Information Management System; and/or

6.14.6 where the Supplier or a Sub-contractor has previously Processed Authority Data that is Personal Data, other than Special Category Personal Data, it proposes to start to Process Authority Data that is Special Category Personal Data under this Contract;

must:

6.14.7 within two Working Days notify the Authority; and

6.14.8 within ten Working Days, or such other timescale as may be agreed with the Authority:

(a) update the Required Changes Register and any other affected parts of the Security Management Plan; and

(b) provide the Authority with a copy of those documents for review and approval.

6.15 Paragraph 6.14 applies in addition to, and not in substitution of, the Parties' obligations to comply with the Change Control Procedure for any Change and with the Change and Evaluation Process for any Service Change.

6.16 Any proposed change under Sub-paragraph 6.14.1, 6.14.2 or 6.14.6 requires a Change to which the Change Control Procedure applies.

6.17 If the Supplier fails to implement a necessary change to the Core Information Management System to address a security-related risk or vulnerability by the date set out in the Required Changes Register:

6.17.1 such failure shall constitute a material Default; and,

6.17.2 the Supplier shall:

(a) immediately – and until the Default is remedied – follow all directions issued by the Authority in writing relating to the Core Information Management System; and

(b) where such material Default is capable of remedy, remedy such material Default within the timescales set by the Authority (considering the security risks the material Default presents to the Services and/or the Supplier Information Management System).

6.18 The Supplier shall review each Change Request against the Security Management Plan to establish whether the documentation would need to be amended should such Change Request be agreed and, where a Change Request would require an amendment to the Security Management Plan, the Supplier shall set out any proposed amendments to the documentation in the Impact Assessment associated with such Change Request for consideration and approval by the Authority.

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 6.19 The Supplier shall be solely responsible for the costs associated with developing and updating the Security Management Plan.

7. Certification Requirements

- 7.1 The Supplier shall ensure, at all times during the Term, that it is certified as compliant with:

7.1.1 ISO/IEC 27001 (at least ISO/IEC 27001:2013) by a UK Accreditation Service (UKAS)-approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013); and

7.1.2 Cyber Essentials Plus,

and shall provide the Authority with a copy of each such certificate of compliance before the Supplier shall be permitted to connect to the Core Information Management System and to receive or Process Authority Data.

- 7.2 Notwithstanding anything else in this Contract, a CIMS Sub-contractor shall be treated for all purposes as a Key Sub-contractor.

- 7.3 In addition to the obligations contained in Clause 15, the Supplier must ensure that the Key Subcontract with each CIMS Sub-contractor contains obligations no less onerous on the Key Sub-contractor than those imposed on the Supplier under this Schedule 5 (*Security Management*).

- 7.4 The Supplier shall ensure that each Higher Risk Sub-contractor is certified as compliant with:

7.4.1 ISO/IEC 27001 (at least ISO/IEC 27001:2013) by a UK Accreditation Service (UKAS)-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013); and

7.4.2 Cyber Essentials Plus,

and shall provide the Authority with a copy of each such certificate of compliance before the Higher-Risk Sub-contractor shall be permitted to receive or Process Authority Data.

- 7.5 The Supplier shall ensure that each Medium Risk Sub-contractor is certified compliant with:

7.5.1 ISO/IEC 27001 (at least 27001:2013) or IASME Assurance Level 2; and

7.5.2 Cyber Essentials Plus.

- 7.6 The Supplier shall ensure that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data:

7.6.1 securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013);

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 7.6.2 should satisfy the Authority that their data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and
 - 7.6.3 must maintain an asset register of all Authority supplied information, data and equipment to ensure Authority assets are returned and/or deleted.
- 7.7 The Supplier shall provide the Authority with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph 7 before the Supplier or the relevant Sub-contractor (as applicable) shall be permitted to carry out the secure destruction of the Authority Data.
- 7.8 The Supplier shall notify the Authority as soon as reasonably practicable, and in any event within three Working Days after becoming aware that in respect any of the certifications required of the Supplier or any Sub-contractor under this Paragraph 7:
 - 7.8.1 such certification has been revoked or cancelled by the body that awarded it;
 - 7.8.2 such certification has expired and has not been renewed by the Supplier or relevant Sub-contractor;
 - 7.8.3 such certification no longer applies to the full scope of the Wider Information Management System; or
 - 7.8.4 the body that awarded such certification has made it subject to conditions, the compliance with which may impact the provision of the Services;(each a "**Certification Default**").
- 7.9 Where the Supplier has notified the Authority of a Certification Default under Paragraph 7.8:
 - 7.9.1 the Supplier shall, within ten Working Days of the date in which the Supplier provided notice under Paragraph 7.8 (or such other period as the Parties may agree) provide a draft plan ("**Certification Rectification Plan**") to the Authority setting out:
 - (a) full details of the Certification Default, including the reasons for the Certification Default;
 - (b) the actual and anticipated effects of the Certification Default in relation to the Services;
 - (c) the steps the Supplier and any Sub-contractor to which the Certification Default relates will take to remedy the Certification Default;
 - 7.9.2 the Authority shall notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Plan;

- 7.9.3 if the Authority rejects the Certification Rectification Plan, the Supplier shall within five Working Days of the date of the rejection submit a revised Certification Rectification Plan and Sub-paragraph 7.9.2 will apply to the re submitted plan;
- 7.9.4 the rejection by the Authority of a revised Certification Rectification Plan is a material Default;
- 7.9.5 if the Authority accepts the Certification Rectification Plan, the Supplier shall start work immediately on the plan, implement it and keep the Authority updated on its progress through to completion.
- 7.10 The Authority may agree to exempt in whole or part the Supplier or any Sub-contractor from the Certification Requirements. Any exemption must be in writing to be effective. The Supplier must include any such exemption in the Security Management Plan.
- 7.11 From the date specified in the Security Management Plan and within 5 Working Days of the end of each subsequent month during the Term, the Supplier shall provide the Authority with a written report which provides in appropriate detail the status of relevant Certifications as required by this Paragraph 7 including their expiry date and associated activities related to their timely renewal.

8. Security Testing

- 8.1 The Supplier shall, at its own cost and expense:
 - 8.1.1 ensure the Core Information Management System has been tested by a CHECK Service Provider (an "**IT Health Check**") within the 12 months prior to the Supplier submitting the Security Management Plan to the Authority for a Security Assurance Decision, unless otherwise agreed by the Authority;
 - 8.1.2 procure the conduct of an IT Health Check on the Core Information Management System once every 12 months during the Term or such other frequency as may be agreed by the Parties;
 - 8.1.3 conduct weekly vulnerability scanning and assessments of the Core Information Management System unless otherwise agreed;
 - 8.1.4 conduct an assessment as soon as reasonably practicable following receipt by the Supplier or any of its Sub-contractors of a critical vulnerability alert from a supplier of any software or other component of the Core Information Management System to determine whether the vulnerability affects the Core Information Management System; and
 - 8.1.5 conduct such other tests as are required by:
 - (a) any Remediation Action Plans;

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (b) the ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification requirements;
- (c) the Security Management Plan; and
- (d) the Authority following a Breach of Security or a significant change to the components or architecture of the Core Information Management System,

(each a “**Security Test**”).

8.2 The Supplier shall provide the Authority with the results of such Security Tests (in a form approved by the Authority in advance) as soon as practicable, and in any case within 10 Working Days, after completion of each Security Test.

8.3 In relation to each IT Health Check conducted under this Paragraph 8, the Supplier shall:

8.3.1 agree with the Authority the aim and scope of the IT Health Check;

8.3.2 promptly, and in any case no later than 10 Working Days, following receipt of each IT Health Check report, provide the Authority with a copy of the IT Health Check report;

8.3.3 in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall (except where Paragraph 8.3.4 applies):

- (a) prepare a remedial plan for approval by the Authority (each a “**Remediation Action Plan**”) which sets out in respect of each vulnerability identified in the IT Health Check report:
 - (i) how the vulnerability will be remedied;
 - (ii) unless otherwise agreed in writing between the Parties, the date by which the vulnerability will be remedied, which must be:
 - (A) within three months of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “medium”;
 - (B) within one month of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “high”;
 - (C) within 7 Working Days of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “critical”;
 - (iii) the tests which the Supplier shall perform or procure to be

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

performed (which may, at the discretion of the Authority, include a further IT Health Check) to confirm that the vulnerability has been remedied;

- (b) comply with the Remediation Action Plan; and
- (c) conduct such further Security Tests on the Core Information Management System to provide independent evidence that the Supplier has complied with the Remediation Action Plan;

8.3.4 where the Supplier can demonstrate to the Authority's reasonable satisfaction that remediation of a vulnerability is not technically feasible or would require disproportionate effort or cost due to the relevant Authority Asset(s) having reached End of Life;

- (a) the Supplier shall record the associated security risks and any mitigations in the Security Management Plan; and
- (b) the Supplier shall not be required to remediate such vulnerability subject to taking all steps agreed under the Residual Risk Statement.

8.4 The Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority. Subject to the Supplier complying with this Paragraph 8.4, if a Security Test causes a Performance Failure in a particular Measurement Period, the Supplier shall be granted relief in respect of such Performance Failure for that Measurement Period.

8.5 The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. Without prejudice to the Supplier's obligations under Paragraph 8.3, the Supplier shall provide the Authority with the results of such Security Tests (in a form approved by the Authority in advance) as soon as practicable, and in any case no later than 10 Working Days, after completion of each Security Test.

8.6 The Authority and/or its authorised representatives shall be entitled, at any time and without giving notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the Core Information Management System and/or the Supplier's compliance with the Security Management Plan ("**Authority Security Tests**"). The Authority shall take reasonable steps to notify the Supplier prior to carrying out such Authority Security Test to the extent that it is reasonably practicable for it to do so taking into account the nature of the Authority Security Test.

8.7 The Authority shall notify the Supplier of the results of such Authority Security Tests after completion of each Authority Security Test.

8.8 The Authority Security Tests shall be designed and implemented so as to minimise their impact on the delivery of the Services. If an Authority Security Test causes Supplier Non-Performance, the Authority Security Test shall be

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

treated as an Authority Cause, except where the root cause of the Supplier Non-Performance was a failure by the Supplier to fulfil any obligation under this Contract.

- 8.9 Without prejudice to the provisions of Paragraph 8.3.3, where any Security Test carried out pursuant to this Paragraph 8 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Authority of any changes to the Core Information Management System and/or the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Authority's prior written approval, the Supplier shall implement such changes to the Core Information Management System and/or the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible.
- 8.10 If the Authority unreasonably withholds its approval to the implementation of any changes proposed by the Supplier to the Security Management Plan in accordance with Paragraph 8.9 above, the Supplier shall not be deemed to be in breach of this Contract to the extent it can be shown that such breach:
- 8.10.1 has arisen as a direct result of the Authority unreasonably withholding its approval to the implementation of such proposed changes; and
- 8.10.2 would have been avoided had the Authority given its approval to the implementation of such proposed changes.
- 8.11 For the avoidance of doubt, where a change to the Core Information Management System and/or the Security Management Plan is required to remedy non-compliance with the Risk Management Documentation, the Baseline Security Requirements and/or any obligation in this Contract, the Supplier shall effect such change at its own cost and expense.
- 8.12 The Supplier shall, by 31 March of each year during the Term, provide to the Authority a letter from its chief information security officer (or equivalent officer) confirming that having made due and careful enquiry:
- 8.12.1 the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters under this Contract; and
- 8.12.2 the Supplier is confident that its security and risk mitigation procedures with respect to the Services remain effective.
- 8.13 From the date specified in the Security Management Plan and within 5 Working Days of the end of each subsequent month during the Term, the Supplier shall provide the Authority with a written report which provides in appropriate detail the status of vulnerabilities identified through IT Health Checks of the Core Information Management System, the elapsed time between the discovery / notification of vulnerabilities their satisfactory remediation, outstanding actions related to mitigation or remediation of public

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

release date of patches, any failure to comply with the timescales set out in Paragraph 8.3 for applying patches to vulnerabilities in the Core Information Management System.

9. Malicious Software

9.1 Unless otherwise agreed the Supplier shall install and maintain Anti-Malicious Software or procure that Anti-Malicious Software is installed and maintained on any part of the Core and Wider Information Management Systems which may Process Authority Data and ensure that such Anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the Core and Wider Information Management Systems to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Core and Wider Information Management Systems, to identify, contain the spread of, and minimise the impact of Malicious Software.

9.2 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

9.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 9.2 shall be borne by the Parties as follows:

9.3.1 by the Supplier where the Malicious Software originates from:

- (a) the Supplier Software;
- (b) the Third-Party Software supplied by the Supplier; or
- (c) the Authority Data whilst the Authority Data is or was under the control of the Supplier,

unless, in the case of the Authority Data, the Supplier can demonstrate that such Malicious Software was present in the Authority Data and not quarantined or otherwise identified by the Authority when the Authority provided the Authority Data to the Supplier; and

9.3.2 otherwise by the Authority.

9.4 From the date specified in the Security Management Plan and within 5 Working Days of the end of each subsequent month during the Term, the Supplier shall provide the Authority with a written report which details the Anti-Malware Software deployment coverage and health based on appropriate metrics including but not limited to compliance with target configuration, positive and false-positive detection rates, and performance.

10. Breach of Security

10.1 If either Party becomes aware of a Breach of Security or an attempted Breach of Security it shall notify the other in accordance with the security incident

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

management process as set out in the Security Management Plan.

- 10.2 The security incident management process set out in the Security Management Plan shall, as a minimum, require the Supplier upon becoming aware of a Breach of Security or an attempted Breach of Security to:

10.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Authority which shall be completed within such timescales as the Authority may reasonably require) necessary to:

- (a) minimise the extent of actual or potential harm caused by such Breach of Security;
- (b) remedy such Breach of Security to the extent possible and protect the integrity of the Core and Wider Information Management Systems against any such potential or attempted Breach of Security;
- (c) apply a tested mitigation against any such Breach of Security or potential or attempted Breach of Security and, provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to deliver the Services so as to meet any Performance Indicator, the Supplier shall be granted relief against the failure to meet such affected Performance Indicator for such period as the Authority, acting reasonably, may specify by written notice to the Supplier; and
- (d) prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure;

10.2.2 as soon as reasonably practicable and, in any event, within 2 Working Days, following the Breach of Security or attempted Breach of Security, provide to the Authority full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.

- 10.3 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security which occurred as a result of non-compliance of the Core or Wider Information Management Systems and/or the Security Management Plan with the Baseline Security Requirements and/or this Contract, then such action and any required change to the Core and/or Wider Information Management Systems and/or Security Management Plan shall be completed by the Supplier at no cost to the Authority.

- 10.4 If the Supplier fails to comply with its obligations set out in this Paragraph 10, such failure shall constitute a material Default, which if not remedied to the satisfaction of the Authority, shall permit the Authority to terminate this Contract in accordance with Clause 31.1(b) with immediate effect by issuing a Termination Notice to the Supplier.

- 10.5 From the date specified in the Security Management Plan and within 5

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Working Days of the end of each subsequent month during the Term, the Supplier shall provide the Authority with a written report which details incidents related to Breach of Security over time, associated incident record identifiers, problem record identifiers, Required Change identifiers, the latest status and next action such that any Breach of Security is appropriately tracked and visible through Reporting.

11. Data Processing, Storage, Management and Destruction

- 11.1 The Supplier's obligations in respect of Processing Personal Data and compliance with the Data Protection Legislation are set out in Clause 21.
- 11.2 The Supplier shall Process Authority Data (that is not Personal Data) only in the UK, except where the Authority has given its consent in writing to a transfer of the Authority Data to such other country (including transfers to countries in the European Economic Area); such consent may be subject to conditions set by the Authority.
- 11.2A The Authority acknowledges that it may require the Supplier to use Authority Assets in the provision of the Services. If such Authority Assets are hosted outside of the UK and therefore the use of such Authority Assets by the Supplier would constitute a transfer of Authority Data outside of the UK, the Authority hereby consents to such transfer.
- 11.3 In addition to the obligations on the Supplier set out in Clause 21 and Paragraph 11.2, the Supplier shall:
 - 11.3.1 on demand, provide the Authority with all Authority Data in an agreed open format;
 - 11.3.2 have documented processes to guarantee availability of Authority Data in the event of the Supplier ceasing to trade;
 - 11.3.3 securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority other than in relation to Authority Data which is owned or licenced by the Supplier or in respect of which the Parties are either Independent Controllers or Joint Controllers; and
 - 11.3.4 securely destroy all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in this Contract and, in the absence of any such requirements, as directed by the Authority other than in relation to Authority Data which is owned or licenced by the Supplier or in respect of which the Parties are either Independent Controllers or Joint Controllers.
- 11.4 In addition to the obligations on the Supplier set out in Clause 21 and Paragraph 11.2, the Supplier shall in relation to all Authority Data except for the Authority's network traffic:
 - 11.4.1 on demand, provide the Authority with all such Authority Data held by the Supplier/Sub-contractor in an agreed open format; and

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 11.4.2 ensure, and must ensure that all Sub-contractors ensure, that such Authority Data is encrypted:
- (a) when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and
 - (b) when transmitted.
- 11.5 Where the Supplier, or a Sub-contractor, cannot encrypt relevant Authority Data as required by sub-Paragraph 11.4.2, the Supplier shall:
- 11.5.1 immediately inform the Authority of the subset or subsets of the relevant Authority Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
 - 11.5.2 provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the relevant Authority as encryption;
 - 11.5.3 provide the Authority with such additional information relating to the information provided under sub-Paragraphs 11.5.1 and 11.5.2 as the Authority may require.
- 11.6 The Parties shall meet to agree appropriate protective measures for the unencrypted Authority Data, and the Supplier shall use reasonable endeavours to procure that relevant Sub-contractors meet the Parties for such purposes where requested by the Authority.
- 11.7 Where the Parties reach agreement on protective measures under Paragraph 11.6, the Supplier shall update the Security Management Plan to include:
- 11.7.1 the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and
 - 11.7.2 the protective measure that the Supplier and/or Sub-contractor will put in place in respect of the unencrypted Authority Data.
- 11.8 Where the Authority and Supplier do not reach agreement on protective measures under Paragraph 11.6 within 40 Working Days of the date on which the Supplier first notified the Authority that it could not encrypt certain relevant Authority Data, either Party may refer the matter to be determined by an expert in accordance with the Dispute Resolution Procedure
- 11.9 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that it shall:
- 11.9.1 in the implementation of cryptographic protections controls, use known public standards and trusted cryptographic technologies; and
 - 11.9.2 utilise cryptographic key management controls to protect the confidentiality, integrity, and availability of keys and trust chains.

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

12. Security Monitoring and Reporting

12.1 The Supplier shall:

- 12.1.1 prepare and submit security reports to the Authority, the frequency and nature of which shall be as detailed and agreed in the Security Management Plan;
- 12.1.2 provide evidence of the presence and effectiveness of controls to the Authority upon request as required to meet through-life Security Assurance, in a format required by the Authority.

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 1: BASELINE SECURITY REQUIREMENTS

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2. Risk management

2.1. The Parties recognise the necessity for risk management and that effective risk management controls are essential to meeting regulatory and contractual obligations.

2.2. The Supplier shall ensure that:

- 2.2.1. systems and data are categorised in line with Government Security Classifications and relevant Laws as applicable;
- 2.2.2. any security risks relating to systems and services that are in control of the Supplier and/or Sub-contractors pursuant to the delivery of the Services are identified and documented;
- 2.2.3. any risks identified in Paragraph 2.2.2 in relation to the Core Information Management System are assessed in accordance with Government risk management practices, Authority risk management practices and together with the Authority Representative and/or relevant Boards to ensure that such risks are understood by identified owners, scored appropriately, and have agreed mitigation and remediation plans, or are otherwise formally accepted by the Authority;
- 2.2.4. security risk assessments are routinely reviewed and updated upon identifying new security vulnerabilities, including using outside sources for security vulnerability information;
- 2.2.5. all Supplier Personnel engaged in the delivery, support, or operation of the Core Information Management System and/or who Process Authority Data have knowledge of the Statement of Information Risk Appetite (SIRA) (if issued) and risk management responsibilities; and
- 2.2.6. supply chain risks associated with the development, acquisition, maintenance and disposal of systems, system components and services, are assessed and managed including documenting of selected mitigating actions and monitoring and reporting performance against those planned actions.

2.3. The Parties acknowledge that any security risks which may arise from:

- 2.3.1. Changes and/or Service Changes to the Gateway System required by the Authority; and/or

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

2.3.2. [REDACTED]

require assessment and control.

2.4. [REDACTED]

3. Data Classification and Handling

- 3.1. The Supplier shall ensure that it makes known Government Security Classifications and the classification of, and associated handling requirements for, Authority Data Processed by the Supplier and/or Sub-contractors to all Supplier Personnel involved in Processing.
- 3.2. If the provision of the Services requires the Supplier to Process Authority Data which is classified as:
- 3.2.1. OFFICIAL-SENSITIVE, the Supplier shall comply with any handling instructions provided with the relevant Authority Data; and/or
- 3.2.2. SECRET or TOP SECRET, the Supplier shall only do so where it has notified the Authority prior to receipt, or if such prior notification is not possible then immediately upon receipt, of such Authority Data and the Supplier shall implement additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.
- 3.3. In respect of digital and non-digital media used for Processing (including storage) of Authority Data, the Supplier shall:
- 3.3.1. control and restrict access to such media to authorised individuals only;
- 3.3.2. protect and control such media during transport outside of controlled areas using appropriate security measures; and
- 3.3.3. sanitise digital media with the strength and integrity commensurate with the classification or sensitivity of the Authority Data prior to disposal, release out of organisational control or release for reuse, in line with published Authority guidance on the topic of secure disposal which can be found at: <https://security-guidance.service.justice.gov.uk/secure-disposal-of-it-public-and-private-cloud/#secure-disposal-of-it---public-and-private-cloud>
- 3.4. The Supplier shall ensure that Authority guidance on data handling and sharing found at: <https://security-guidance.service.justice.gov.uk/data-handling-and-information-sharing-guide/#data-handling-and-information-sharing-guide> is known to and followed by all Supplier Personnel involved in Processing.

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 3.5. The Supplier shall ensure that processes are in use to assist in making information-sharing decisions to ensure data is appropriately protected, and mechanisms exist to secure *ad hoc* exchanges of large digital files with authorised parties in line with the standards, Authority guidance and Good Industry Practice.
- 3.6. The Supplier shall ensure that processes are in place to inventory, document and maintain Documentation of data flows for Authority Data that is resident within the Services' distributed applications, infrastructure, and system components.
- 3.7. The Supplier shall ensure that media and Authority Data are retained in accordance with applicable statutory, regulatory, and contractual obligations.

4. Location of Authority Data

- 4.1. The Parties recognise the need for the Authority's information to be safeguarded under the UK Data Protection regime or a similar regime. The Supplier must be able to state to the Authority the physical locations in which Authority Data may be Processed (including stored) and managed from, and what legal and regulatory frameworks Authority Data will be subject to at all times.
- 4.2. The Supplier's obligations in respect of Processing Personal Data and compliance with the Data Protection Legislation are set out in Clause 21. The Supplier shall and shall procure that its Sub-contractors shall only Process Authority Data (that is not Personal Data) in the UK, except where the Authority has given its consent in writing to a transfer of the Authority Data to such other country (including transfers to countries in the European Economic Area), which may be subject to conditions.
- 4.3. The Supplier shall agree any change in location of Processing and administration of Authority Data with the Authority in accordance with the Change Control Procedure, and in accordance with Clause 21 (Protection of Personal Data) if the change relates to the Processing of Personal Data.

5. Data Destruction or Deletion

- 5.1. The Supplier shall:
- 5.1.1. prior to securely sanitising any Authority Data, or when requested to do so by the Authority, provide the Authority with all Authority Data in an agreed open format;
 - 5.1.2. have documented processes to ensure the availability of Authority Data in the event of the Supplier ceasing to trade;
 - 5.1.3. securely erase in a manner agreed with the Authority any or all Authority Data held by the Supplier when requested to do so by the Authority;

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 5.1.4. securely destroy in a manner agreed with the Authority all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in this Contract and, in the absence of any such requirements, as agreed by the Authority; and
- 5.1.5. document and implement processes agreed by the Authority which address the NCSC guidance on secure sanitisation.

6. End User Devices

- 6.1. The Supplier must manage, and must ensure that all Sub-contractors manage, effective security controls on all end-user devices used by the Supplier (and Sub-contractors) on which Authority Data is Processed in accordance the following requirements:
 - 6.1.1. the operating system and any applications that Process or have access to Authority Data must be in current support by the vendor, or the relevant community in the case of Open-Source operating systems or applications;
 - 6.1.2. users must authenticate before gaining access;
 - 6.1.3. all Authority Data must be encrypted using an encryption tool agreed to by the Authority;
 - 6.1.4. the end-user device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the end-user device is inactive;
 - 6.1.5. the end-user device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Authority Data to facilitate continuous enforcement and reporting on configuration compliance;
 - 6.1.6. the Supplier or Sub-contractor, as applicable, can, without physical access to the end-user device, remove or make inaccessible all Authority Data on the device and prevent any user or group of users from accessing the device;
 - 6.1.7. all end-user devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification issued by a UKAS-approved certification body where the scope of that certification includes the Services;
 - 6.1.8. the end-user device must utilise anti-malware technologies to detect and eradicate malicious code.
- 6.2. The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance, as they are updated, amended or replaced on an ongoing basis, as if those recommendations were incorporated as specific obligations under this Agreement.

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 6.3. Where there is any conflict between the requirements of this Schedule 5 (*Security Management*) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.

7. Encryption

- 7.1. The Supplier must ensure, and must ensure that all Sub-contractors ensure, that:
- 7.1.1. Authority Data is encrypted when stored at any time when no operation is being performed on it;
 - 7.1.2. Authority Data is encrypted when transmitted;
 - 7.1.3. in the implementation of cryptographic protections controls, known public standards and trusted cryptographic technologies are used; and
 - 7.1.4. cryptographic key management controls to protect the confidentiality, integrity, and availability of keys and trust chains are utilised.
- 7.2. Where the Supplier, or a Sub-contractor, cannot encrypt Authority Data the Supplier must:
- 7.2.1. immediately inform the Authority of the subset or subsets of Authority Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
 - 7.2.2. provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and
 - 7.2.3. provide such other information as the Authority may require relating to the Authority Data concerned.
- 7.3. The Parties and, where the Authority requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Authority Data.
- 7.4. Where the Authority and Supplier reach agreement, the Supplier must update the Security Management Plan to include:
- 7.4.1. the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and
 - 7.4.2. the protective measure that the Supplier and/or Sub-contractor will put in place in respect of the unencrypted Authority Data.
- 7.5. Where the Parties do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Authority that it could not encrypt certain Authority Data, either Party may refer the matter to be determined in accordance with the Dispute Resolution Procedure.

8. Personnel Security

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 8.1. All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record.
- 8.2. The Parties shall review the roles and responsibilities of Supplier Personnel who will be involved in the management and/or provision of the Services in order to enable the Authority to determine the required level of national security vetting clearance per role in accordance with the Cyber and Technical Security Guidance published at <https://security-guidance.service.justice.gov.uk/#cyber-and-technical-security-guidance>.
- 8.3. The Supplier shall not permit Supplier Personnel who fail the security checks required by Paragraph 8.1 and/or fail to meet the clearance requirements of Paragraph 8.2 to be involved in the management and/or provision of the Services except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.
- 8.4. The Supplier shall ensure that Supplier Personnel are only granted such access to Authority Data as is necessary to enable the Supplier Personnel to perform their role and to fulfil their responsibilities.
- 8.5. The Supplier shall ensure that Supplier Personnel who no longer require access to Authority Data (e.g. they cease to be employed by the Supplier or any of its Sub-contractors) have their rights to access Authority Data revoked as soon as practicable.
- 8.6. The Supplier shall ensure that processes are in place to govern and manage data access controls upon the termination of individual employment of Supplier Personnel.
- 8.7. The Supplier shall ensure that Supplier Staff that have access to the Sites, the IT Environment or the Authority Data receive regular training on security awareness that reflects the degree of access those individuals have to the Sites, the IT Environment or the Authority Data.
- 8.8. The Supplier shall ensure that the training provided to Supplier Staff under Paragraph 8.7 includes training on the identification and reporting of fraudulent communications intended to induce individuals to disclose Personal Data or any other information that could be used, including in combination with other Personal Data or information, or with other techniques, to facilitate unauthorised access to the Sites, the IT Environment or the Authority Data ("phishing").
- 8.9. The Supplier shall implement and maintain separation of duties where appropriate, including to prevent potential inappropriate activity.
- 8.10. The Supplier shall ensure all Supplier Personnel to apply cybersecurity and privacy principles in their daily work.

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

9. Identity, Authentication and Access Control

- 9.1. The Supplier shall operate an identification and access management control regime to ensure:
- 9.1.1. all users, administrators and processes, including any third-party users and processes, are uniquely identified and centrally authenticated, authorised, and audited when accessing or administering the Services;
 - 9.1.2. all persons who access the Sites are identified and authenticated before they are allowed access to the Sites;
 - 9.1.3. all devices are uniquely identified, and centrally authenticated, authorised, and audited before establishing a connection, which must be cryptographically based and replay-resistant;
 - 9.1.4. mechanisms are in place at all times to identify and authenticate any third-party systems and services;
 - 9.1.5. mechanisms are in place at all times to securely manage authenticators for users and devices; and
 - 9.1.6. identifiers are not shared or re-used between environments.
- 9.2. The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) when allowing or configuring access to the Supplier System, the Gateway System and Sites so that such access is only to those parts of the Sites and the Supplier System and the Gateway System that the relevant Supplier Personnel require to accomplish assigned tasks.
- 9.3. The Supplier shall ensure that role-based access control (RBAC) policy over users and resources applies need-to-know and fine-grained access control, enforcing principles of least privilege.
- 9.4. The Supplier shall retain records of access to the Sites and to the Supplier System and the Gateway System and shall make such records available to the Authority on request.
- 9.5. The Supplier shall enforce multi-factor authentication (MFA) where published guidance demands or recommends it and for remote network access, third party systems, applications and/or services, and/or for non-console privileged access to systems.
- 9.6. The Supplier shall pro-actively govern account management of all accounts including user, privileged user, and non-user accounts, utilising registration and de-registration processes to govern the assignment of user rights.
- 9.7. The Supplier shall periodically (at least every 3 months) review the privileges assigned to user and non-user accounts to validate the need for such privileges, reassign or remove unnecessary privileges as necessary, and provide appropriate associated reporting to the Authority illustrating control over access, privileged access, and granted privileges.

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

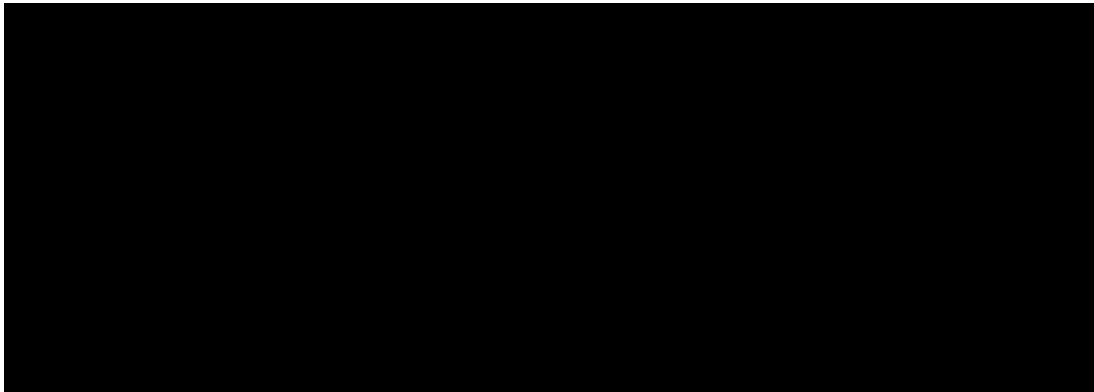
Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

10. Audit and Protective Monitoring

- 10.1. The Supplier shall make available to the Authority audit records which relate to security Events in the Core Information Management System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness, such audit records shall (as a minimum and to the extent supported by the Core Information Management System) include regular reports and alerts setting out details of access by users of the Core Information Management System, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data.
- 10.2. The Supplier shall support any response initiated by the Authority to indicators of system or account compromise, indicators of unauthorised exfiltration of non-public information, and other potentially malicious activities.
- 10.3. The Core Information Management System must be configured by the Supplier to, at a minimum and to the extent supported by the Core Information Management System, generate audit records for system Events, authorisation Events, failure or error-related Events, and all security operations and functions.
- 10.4. The Core Information Management System must be configured by the Supplier (to the extent supported by the Devices) such that audit records contain sufficient information to meet the "MoJ Cyber and Technical Security Guidance" Standard and:



- 10.5. The Supplier shall protect the confidentiality, integrity, and availability of Event logs within its control by:
- 10.5.1. not used;
 - 10.5.2. alerting the Authority in the event of a log processing failure;
 - 10.5.3. protecting logs from unauthorised access, modification, or deletion; and
 - 10.5.4. configuring systems to use an authoritative time source synchronised with the Master Time Reference to generate time stamps for logs.
- 10.6. The Supplier shall make available to the Authority audit records generated by or pertaining to access to the Core Information Management System, such that the Authority may perform direct analysis of recorded Events.

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

10.7. The Supplier shall ensure that audit data made available to the Authority under this Paragraph 10 are transmitted in near-real time either to the Authority's cybersecurity log platform or to the Authority's syslog collector and/or VM broker.

11. Security Operations

11.1. The Supplier shall implement operational security controls to:

11.1.1. define and deliver capabilities supporting the Authority based on Good Industry Practice to meet the Authority's service needs; and

11.1.2. to utilise and collaborate with the capabilities available through the Authority's security operations centre.

12. Threat Management

12.1. The Supplier shall monitor threat intelligence sources as part of day to day operations related to the security of the Services, and notify the Authority of any threat intelligence information that may influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.

12.2. The Supplier shall develop and maintain a documented understanding of potential attack vectors that could be used to attack the Core Information Management System through Risk Assessment contained in the Security Management Plan.

12.3. The Supplier shall ensure that it is able to maintain situational awareness of evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the recommendation and subsequent implementation of preventative and compensating controls.

13. Information Assurance

13.1. The Supplier shall:

13.1.1. facilitate the implementation and use of data privacy impact assessments and relevant authorisation controls, including use of the Authority's privacy assessment and authorisation controls;

13.1.2. formally assess the cybersecurity and privacy controls of the Supplier System and Gateway System and Licensed Software periodically, to determine the extent to which the controls are implemented correctly, operating as intended, producing the desired outcomes and meeting expected requirements;

13.1.3. maintain in the Virtual Library key architectural Documentation and information on each critical system, application or service. Such Documentation shall utilise Good Industry Practice and shall be suitable for influencing inputs, entities, systems, applications and processes, and for use as Records of the relevant data and its origins;

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 13.1.4. evaluate the design, implementation and effectiveness of technical cybersecurity and privacy controls relating to the Services; and
- 13.1.5. ensure systems, projects and services are formally authorised by the Authority prior to being implemented by the Supplier in the IT Environment and/or Operating Environment.

14. Physical and Environmental Security

- 14.1. Where physical and environmental security is in the control of the Supplier or Sub-Contractor, the Supplier shall ensure that:
 - 14.1.1. mechanisms are in place to facilitate the operation of proportionate physical and environmental protection controls; and
 - 14.1.2. physical access control mechanisms are in place to maintain a current list of Supplier Personnel and personnel of the Authority with authorised access to facilities (except for those areas within the facility officially designated as publicly accessible).

15. Project and Resource Management

- 15.1. The Supplier shall ensure that Changes, Operational Changes and Service Changes are impact-assessed from a security perspective, to ensure that vulnerabilities are not introduced and that the Security Management Plan can be updated in a timely manner to accommodate changes which impact the Security Management Plan.
- 15.2. The Supplier shall operate effective knowledge management for all Supplier Personnel responsible for cybersecurity and privacy, regarding knowledge of the Authority's and the Service Recipients' operational needs as required for effective security management.

16. Security Awareness and Training

- 16.1. The Supplier shall facilitate the implementation of security workforce development and awareness controls to:
 - 16.1.1. provide all Supplier Personnel with appropriate security awareness education and training that is relevant for their job function;
 - 16.1.2. provide role-based security-related training before authorising access to the system or performing assigned duties, when required by system changes, and annually thereafter; and
 - 16.1.3. document, retain and monitor individual training activities, including basic security awareness training, ongoing awareness training and specific-system training.

17. Vulnerability and Patch Management

- 17.1. The Parties acknowledge that vulnerabilities in the Core Information Management System may be discovered which unless mitigated will present an

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

unacceptable risk to the Authority Data, and that the implementation and monitoring of effective vulnerability management controls are critical to protecting confidentiality, integrity and availability.

- 17.2. The Supplier shall ensure that controls are implemented in the Core Information Management System to ensure that vulnerabilities are properly identified, tracked, and remediated during the Term.
- 17.3. The Supplier shall ensure that mechanisms are in place to detect vulnerabilities and configuration errors in the Core Information Management System by recurring vulnerability scanning of systems.
- 17.4. The severity of vulnerabilities for Gateway Device Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the method described in the Security Management Plan and using the appropriate vulnerability scoring systems including the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'Critical', 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST at <http://nvd.nist.gov/cvss.cfm>).
- 17.5. Subject to Paragraph 17.6 the Supplier shall procure the application of security patches to vulnerabilities in the Core Information Management System within:
- 17.5.1. seven (7) days after the public release of patches for those vulnerabilities categorised as 'Critical';
 - 17.5.2. thirty (30) days after the public release of patches for those vulnerabilities categorised as 'High' ; and
 - 17.5.3. sixty (60) days after the public release of patches for those vulnerabilities categorised as 'Medium' or 'Low'.
- 17.6. The Supplier shall ensure all patches planned for release are tested in accordance with Release and Deployment Management, and deployed in accordance with the Change and Evaluation Management Process.
- 17.7. The timescales for applying patches to vulnerabilities in the Core Information Management System set out in Paragraph 17.5 shall be extended by the Authority if:
- 17.7.1. the Supplier can demonstrate that a vulnerability in the Core Information Management System is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the timescales set out in Paragraph 17.5 if the vulnerability becomes exploitable within the context of the Services;
 - 17.7.2. the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days,

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or

17.7.3. the Authority agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Security Management Plan.

17.8. The Security Management Plan shall include provisions for all Gateway Device Software to be kept up-to-date, such that all Gateway Device Software shall always be in mainstream or extended security support throughout the Term and not more than one version or major release behind the latest version unless otherwise agreed by the Authority in writing.

17.9. The Supplier shall not release any software (including update) to the IT Environment and/or Operating Environment without evidence of a current vulnerability scan, associated mitigations, or documented exemption(s) approved by the Authority.

17.10. In addition to the Security Tests, the Supplier shall:

17.10.1. specify in the Security Management Plan the scope of the Core Information Management System to be CHECK tested;

17.10.2. at its own cost and expense, procure and conduct tests to the Core Information Management System in accordance with the Security Management Plan;

17.10.3. at its own cost and expense (unless otherwise agreed), procure and conduct such other security tests as may be required by the Authority in order to provide necessary assurances that effective controls are in place; and

17.10.4. provide the Authority with the full results of the tests conducted under Sub-paragraphs 17.10.2 and/or 17.10.3, promptly following the completion of each such test.

17.11. The frequency of the tests required under Sub-Paragraph 17.10.2 shall be once per Contract Year or as may be otherwise more frequently specified in the Security Management Plan.

17.12. The Supplier shall report to the Authority within the Performance Management Report (or such other monthly report as may be agreed by the Authority from time to time):

17.12.1. patched and outstanding vulnerabilities in the Core Information Management System (to the extent that the Core Information Management System is within the control of the Supplier);

17.12.2. any elapsed time from the public release date of patches to the patches being applied;

17.12.3. either the date of application or, for outstanding vulnerabilities, the planned date; and

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 17.12.4. proposed interim mitigation measures for vulnerabilities in the managed environment which are known to be exploitable, where a security patch is not immediately available.

18. Asset Management

18.1. The Supplier must manage, and ensure that all Sub-contractors manage, all Authority Assets such that:

- 18.1.1. Authority Assets are inventoried in the ITSM Toolset to accurately reflect the current systems, applications, and services;
- 18.1.2. asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organisation level;
- 18.1.3. network and solution architecture diagrams are maintained, with sufficient detail to assess the security and reflect the current architecture;
- 18.1.4. sanctions that require the removal and prohibition of certain technology services and/or equipment that are designated as threats by a statutory or regulatory body are implemented; and
- 18.1.5. proper decommissioning processes for systems, applications and services are used, so that Authority Data is properly transitioned to new systems or archived in accordance with applicable organisational standards, as well as statutory, regulatory and contractual obligations, and that information is prevented from being recovered from decommissioned components following secure disposal, destruction, or repurposing.

19. Configuration Management

19.1. The Supplier shall ensure:

- 19.1.1. configuration management controls are in use;
- 19.1.2. develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards;
- 19.1.3. configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services;
- 19.1.4. restrict the ability of non-privileged users to install unauthorised software; and
- 19.1.5. obtain, protect, maintain, update, and distribute administrator documentation that describe:
- 19.1.6. secure configuration, installation and operation; and
- 19.1.7. effective use and maintenance of security features/functions.

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

20. Maintenance

20.1. The Supplier must ensure:

- 20.1.1. mechanisms are in place to develop, disseminate, review and update procedures to facilitate the implementation and validation of maintenance controls related to the Core Information Management System;
- 20.1.2. processes are in place to protect the authenticity, confidentiality, integrity, and availability of assets during maintenance activities impacting the Core Information Management System;
- 20.1.3. mechanisms are in place to authorise, monitor, and control all maintenance and diagnostic activities, including any remote maintenance, and including any associated transfer and storage;
- 20.1.4. proper physical security and configuration control over Authority Assets awaiting service or repair; and
- 20.1.5. the use of system maintenance tools within the Core Information Management System is controlled and monitored by the Supplier.

21. Security Incident Response

21.1. The Supplier shall:

- 21.1.1. implement and govern processes and Documentation to facilitate a response capability for Security Incidents, including to meet the Performance Levels;
- 21.1.2. respond to all Security Incidents as raised to the Supplier by the Authority;
- 21.1.3. put in place the capabilities to identify and pro-actively manage the Core Information Management System against Security Incidents;
- 21.1.4. document, monitor and report the status of Security Incidents to the Authority all the way through to Resolution (as defined in Schedule 3 (*Performance Levels*)) of each Security Incident;
- 21.1.5. ensure a viable and current Security Incident response process is documented in the Security Management Plan covering the intake of Security Incident reporting, analysis, eradication and recovery;
- 21.1.6. ensure an integrated (virtual) team of cybersecurity, IT, and business function representatives appropriate and proportional to the purposes of the Security Incident response function and appropriate to the Services is defined and maintained in the Security Management Plan;
- 21.1.7. ensure Supplier Personnel are provided with guidance and/or training by the Supplier in their Security Incident response roles and responsibilities;

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 21.1.8. formally test Security Incident response capabilities periodically through realistic exercises to determine the operational effectiveness of those capabilities;
- 21.1.9. document, monitor and report the status of Security Incidents to internal stakeholders, affected third parties and where, required to do so by Law, regulatory authorities, through to Resolution (as defined in Schedule 3 (*Performance Levels*)) of the Security Incident;
- 21.1.10. ensure documented processes agreed by the Authority are in place to facilitate a rapid and secure response to any security investigation undertaken by the Authority;
- 21.1.11. ensure that the integrity of data which might subsequently be relied upon in Court shall be maintained throughout a forensic investigation process; and
- 21.1.12. ensure documented processes are defined and followed by the Supplier so that lessons are learned from analysing and resolving Security Incidents to reduce the likelihood or impact of future Security Incidents.

22. Compliance**22.1. The Supplier must:**

- 22.1.1. facilitate the identification and implementation of relevant statutory, regulatory, and contractual controls;
- 22.1.2. operate a security and privacy controls oversight function that reports to its executive leadership;
- 22.1.3. ensure its managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate security policies, standards and other applicable requirements;
- 22.1.4. maintain all relevant certifications with appropriate accredited bodies; and
- 22.1.5. support the Authority in meeting legal and regulatory obligations, including data protection impact assessments (DPIAs), Requests for Information and subject access requests (SARs), Departmental Security Health Check (DSHC) and other authorised compliance audits.

23. Secure Engineering and Architecture

- 23.1. The Supplier shall utilise Good Industry Practice cybersecurity and privacy approaches and principles that address risk to organisational operations, assets, individuals, and other organisations in the specification, design, development, implementation and modification of systems and services in accordance with:

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 23.1.1. Cyber and Technical Security Guidance, a copy of which can be found at <https://security-guidance.service.justice.gov.uk/#cyber-and-technical-security-guidance>;
- 23.1.2. HMG Secure by Design, a copy of which can be found at: <https://www.security.gov.uk/guidance/secure-by-design/> and NCSC Cyber Assessment Framework a copy of which can be found at <https://www.ncsc.gov.uk/collection/caf>
- 23.1.3. NCSC guidance which can be found at: <https://www.ncsc.gov.uk/section/advice-guidance/all-topics>;
- 23.1.4. the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main>;
- 23.1.5. the NCSC "Bulk Data Principles", a copy of which can be found at <https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main>; and
- 23.1.6. the NCSC "Cloud Security Principles", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles> and which are summarised below:
- (a) "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;
 - (b) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;
 - (c) "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;
 - (d) "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Services and information within it;
 - (e) "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;
 - (f) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Personnel have access to Authority Data and/or the Authority System that those

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

personnel be subject to appropriate security screening and regular security training;

- (g) "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;
- (h) "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Sub-contractors and other suppliers;
- (i) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Authority to securely manage the Authority's use of the Service;
- (j) "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;
- (k) "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;
- (l) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;
- (m) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Authority with the audit records it needs to monitor access to the Service and the Authority Data held by the Supplier and/or its Sub-contractors; and
- (n) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Personnel on the safe and secure use of the Information Management System.

23.2. The Supplier shall ensure that all critical system clocks shall be synchronised with the Master Time Reference.

23.3. To the extent that the Supplier is responsible for solution design, such design shall take account of all controls (e.g. segregation) necessary for the protection of Authority Data and the Services, in accordance with the SIRA (if a SIRA has been shared), from vulnerabilities including those which may arise during development, testing and Release Management.

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

23.4. The Supplier shall notify the Authority of any insufficiency (or risk of insufficiency) of the controls required under Paragraph 23.3.

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 2: SECURITY REQUIREMENTS FOR SUB-CONTRACTORS**1 Application of Annex 2**

- 1.1 This Annex 2 applies to all Sub-contractors that Process Authority Data.
- 1.2 The Supplier must:
 - (a) ensure that those Sub-contractors comply with the provisions of this Annex 2;
 - (b) keep sufficient records to demonstrate that compliance to the Authority; and
 - (c) ensure that its Implementation Plan includes Deliverable Items, Milestones and Milestone Dates that relate to the design, implementation and management of any systems used by Sub-contractors to Process Authority Data.

2 Designing and managing secure solutions

- 2.1 The Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a NCSC Certified Professional certification for all bespoke or complex components.
- 2.2 The Sub-contractor shall implement their solution(s) to mitigate the security risks in accordance with;
 - (a) NCSC's Cyber Security Design Principles
<https://www.ncsc.gov.uk/collection/cyber-security-design-principles>; and
 - (b) NCSC Cyber Assessment Framework (CAF).
<https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance>
- 2.3 The Sub-contractor must assess their systems against the NCSC Cloud Security Principles: <https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles> at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-contractor must document that assessment and make that documentation available to the Authority on the Authority's request.

3 Data Processing, Storage, Management and Destruction

- 3.1 The Supplier shall ensure that Authority Data is protected and Processed in a secure manner. To achieve this objective, the Authority Data shall only be Processed within the United Kingdom subject to Paragraph 11.1 of Schedule 5. The Supplier must align with UK Data Protection Legislation, MoJ Cyber and Technical Security Guidance, NCSC Cyber Assessment Framework Guidance, and all NCSC guidance on Cyber Security to ensure the security and protection of the Authority Data. In addition, appropriate measures must be put in place to prevent unauthorised access, use, or disclosure of the Authority Data. The Supplier shall agree under the Change Control Procedure,

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

any change in location of Processing and / or administration of Authority Data (in accordance with Clause 21 (Protection of Personal Data) if the Change relates to the Processing of Personal Data).

3.2 The Sub-contractor must, when requested to do so by the Authority:

- (a) securely destroy Authority Data only on Sites which are included within the scope of an existing ISO/IEC 27001 certification;
- (b) satisfy the Authority that their data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and
- (c) maintain an asset register of all Authority supplied information, data and equipment to ensure Authority assets are returned and/or deleted.

4 Personnel Security

4.1 The Sub-contractor must perform appropriate checks on their staff before they may participate in the provision and or management of the Services. Those checks must include all pre-employment checks required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record. The HMG Baseline Personnel Security Standard can be found at: <https://www.gov.uk/government/publications/government-baseline-personnel-security-standard>.

4.2 The Sub-contractor must, if the Authority requires, at any time, ensure that one or more of the Sub-contractor's staff obtains Security Check clearance in order to Process Authority Data containing Personal Data above certain volumes specified by the Authority, or containing Special Category Personal Data.

4.3 Any Sub-contractor staff who will, when performing the Services, have access to a person under the age of 18 years must undergo Disclosure and Barring Service (DBS) checks.

5 End User Devices

5.1 The Supplier must manage, and must ensure that all Sub-contractors manage, all end-user devices used by the Supplier on which Authority Data is Processed in accordance the following requirements:

- a) the operating system and any applications that Process or have access to Authority Data must be in current support by the vendor, or the relevant community in the case of Open Source operating systems or applications;
- b) users must authenticate before gaining access;
- c) all Authority Data must be encrypted using an encryption tool agreed to by the Authority;

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- d) the end-user device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the end-user device is inactive;
 - e) the end user device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Authority Data to facilitate continuous enforcement and reporting on configuration compliance;
 - f) the Supplier or Sub-contractor, as applicable, can, without physical access to the end-user device, remove or make inaccessible all Authority Data on the device and prevent any user or group of users from accessing the device;
 - g) all end-user devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services provided in relation to the contract.
 - h) mechanisms are in in place at all times to utilise anti-malware technologies to detect and eradicate malicious code.
- 5.2 The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance, as they are updated, amended or replaced on an ongoing basis, as if those recommendations were incorporated as specific obligations under this Agreement.
- 5.3 Where there any conflict between the requirements of this Schedule 5 (*Security Management*), and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.

6 Not used**7 Patching and Vulnerability Scanning**

- 7.1 The Sub-contractor must proactively monitor supplier vulnerability websites and ensure all necessary patches and upgrades are applied to maintain security, integrity and availability in accordance with the Patch Management Guide (<https://security-guidance.service.justice.gov.uk/patch-management-guide/#patch-management-guide>), and the NCSC Cloud Security Principles.

8 Third Party Sub-contractors

- 8.1 The Sub-contractor must not transmit or disseminate the Authority Data to any other person unless specifically authorised by the Authority. Such authorisation must be in writing to be effective and may be subject to conditions.
- 8.2 The Sub-contractor must not, when performing any part of the Services, use any software to Process the Authority Data where the licence terms of that

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

software purport to grant the licensor rights to Progress the Authority Data
greater than those rights strictly necessary for the use of the software

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 3: SECURITY MANAGEMENT PLAN TEMPLATE**Security Management Plan Template****[Project/Service and Supplier Name]****1 Executive Summary**

<This section should contain a brief summary of the business context of the system, any key IA controls, the assurance work done, any off-shoring considerations and any significant residual risks that need acceptance.>

2. System Description**2.1 Background**

< A short description of the project/product/system. Describe its purpose, functionality, aim and scope.>

2.2 Organisational Ownership/Structure

<Who owns the system and operates the system and the organisational governance structure. This should include how any ongoing security management is integrated into the governance of the Contract and/or projects; e.g. how a security matters will reported to relevant Boards.>

2.3 Information assets and flows

<The information assets processed by the system which should include a simple high level diagram on one page. Include a list of the type and volumes of data that will be processed, managed and stored within the supplier system. If personal data, please include the fields used such as name, address, department DOB, NI number etc.>

2.4 System Architecture

<A description of the physical system architecture, to include the system management. A diagram will be needed here>

2.5 Users

<A brief description of the system users, to include HMG users as well as any service provider users and system managers. If relevant, security clearance level requirements should be included.>

2.6 Locations

<Where the data assets are stored and managed from. If any locations hold independent security certifications (e.g. ISO27001 (at least ISO/IEC 27001:2013) these should be noted. Any off-shoring considerations should be detailed.>

2.7 Test and Development Systems

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

<Include information about any test and development systems, their locations and whether they contain live system data.>

2.8 Key roles and responsibilities

<A brief description of the lead security roles such as that of the SIRO, IAO, Security manager >

3. Risk Assessment

3.1 Assurance Scope

<This section describes the scope of the Security Assurance for the system. The scope of the assurance assessment should be clearly indicated, with components of the architecture upon which reliance is placed but assurance will not be done clearly shown e.g. a cloud hosting service. A logical diagram should be used along with a brief description of the components.>

3.2 Risk appetite

<A risk appetite should be agreed with the SRO and included here.>

3.3 Business impact assessment

< A description of the information assets and the impact of their loss or corruption (e.g. large amounts of Official Sensitive personal data the loss of which would be severely damaging to individuals, embarrassing to HMG, and make HMG liable to ICO investigations) in business terms should be included. This section should cover the impact on loss of confidentiality, integrity and availability of the assets. The format of this assessment may be dependent on the risk assessment method chosen.>

3.4 Risk assessment

<The content of this section will depend on the risk assessment methodology chosen and should contain the output of the formal information risk assessment in a prioritised list using business language. Experts on the system and business process should have been involved in the risk assessment to ensure the formal risk methodology used has not missed out any risks. The example table below should be used as the format to identify the risks and document the controls used to mitigate those risks. >

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R1	Internet attackers could hack the system.	Medium	The service systems are exposed to the internet via the web portal.	C1: Internet-facing firewalls C2: Internet-facing IP whitelist C3: System hardening	Very low

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
				C4: Protective monitoring C5: Application access control C16: Anti-virus for incoming files C54: Files deleted when processed C59: Removal of departmental identifier	
R2	Remote attackers could intercept or disrupt information crossing the internet.	Medium	File sharing with organisations across the internet.	C9: TLS communications C10: PGP file-sharing	Very low
R3	Internal users could maliciously or accidentally alter bank details.	Medium-High	Users bank details can be altered as part of the normal business function.	C12. System administrators hold SC clearance. C13. All changes to user information are logged and audited. C14. Letters are automatically sent to users' home addresses when bank details are altered. C15. Staff awareness training	Low

3.5 Controls

<The controls listed above to mitigate the risks identified should be detailed. There shall be a description of each control, further information and configuration details where relevant, and an assessment of the implementation status of, and assurance in, the control. A sample layout is included below.>

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ID	Control title	Control description	Further information and assurance status
C1	Internet-facing firewalls	Internet-facing firewalls are in place between the internet and the system', which restrict access from the internet to the required ports only.	Assured via ITHC firewall rule check
C2	Internet-facing IP whitelist	An IP whitelist is in place for all access from the internet.	Assured via ITHC
C15	Staff awareness training	All staff must undertake annual security awareness training and this process is audited and monitored by line managers.	Assured as part of ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification

3.6 Residual risks and actions

<A summary of the residual risks which are likely to be above the risk appetite stated after all controls have been applied and verified should be listed with actions and timescales included.>

4. In-service controls

< This section should describe the controls relating to the information lifecycle, including development, testing, in-service, termination and on-going risk management and assurance. Details of any formal assurance requirements specified in the contract such as security CHECK testing or maintained ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification should be included. This section should include at least:

- (a) information risk management and timescales and triggers for a review;*
- (b) contractual patching requirements and timescales for the different priorities of patch;*
- (c) protective monitoring arrangements to include how anomalous behaviour is identified and acted upon as well as how logging and auditing of user activity is done;*
- (d) configuration and change management;*
- (e) incident management;*
- (f) vulnerability management;*
- (g) user access management; and*
- (h) data sanitisation and disposal.>*

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 5. Security Operating Procedures (SyOPs)**
- < If needed any SyOps requirements should be included and referenced here.>*
- 6. Major Hardware and Software and end of support dates**
- < This should be a table which lists the end of support dates for hardware and software products and components. An example table is shown below.>*

Name	Version	End of mainstream Support/Extended Support	Notes/RAG Status
Server Host	HP XXXX	Feb 2020/ March 2022	

- 7. Incident Management Process**
- <The suppliers' process, as agreed with the Authority/Customer, should be included here. It must as a minimum include the protocol for how and when incidents will be reported to the Authority/customer and the process that will be undertaken to mitigate the incidents and investigate the root cause.>*
- 8. Security Requirements for User Organisations**
- <Any security requirements for connecting organisations or departments should be included or referenced here.>*
- 9. Required Changes Register**
- <The table below shows the headings for the Required Changes Register which should be maintained and used to update the contents of this document at least annually.>*

Ref	Section	Change	Agreed With	Date agreed	Documentation update	Status
1	6.4	A new Third Party supplier XXXX will be performing the print capability.	Authority name	11/11/2018	Jul-2019	Open

- 10. Sub-contractors**
- <This should include a table which shows for each Sub-contractor their name, the function that they are performing, the data and data volume being processed, the location, and their certification status>*
- 11. Annex A. ISO/IEC 27001 (at least ISO/IEC 27001:2013) and/or Cyber Essential Plus certificates**
- <Any certifications relied upon should have their certificates included>*

SCHEDULE 5 (SECURITY MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

12. Annex B. Cloud Security Principles assessment

<A spreadsheet may be attached>

13. Annex C. Protecting Bulk Data assessment if required by the Authority/Customer

<A spreadsheet may be attached>

14. Annex D. Latest ITHC report and Remediation Action Plan

SCHEDULE 6 (INSURANCE REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 6

INSURANCE REQUIREMENTS

SCHEDULE 6 (INSURANCE REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 6 (*Insurance Requirements*)**1 OBLIGATION TO MAINTAIN INSURANCES**

- 1.1 Without prejudice to its obligations to the Authority under this Contract, including its indemnity and liability obligations, the Supplier shall for the periods specified in this Schedule take out and maintain, or procure the taking out and maintenance of the insurances as set out in Annex 1 and any other insurances as may be required by applicable Law (together the “Insurances”). The Supplier shall ensure that each of the Insurances is effective no later than the date on which the relevant risk commences.
- 1.2 The Insurances shall be maintained in accordance with Good Industry Practice and (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time.
- 1.3 The Insurances shall be taken out and maintained with insurers who are:
- (a) of good financial standing;
 - (b) appropriately regulated;
 - (c) regulated by the applicable regulatory body and is in good standing with that regulator; and
 - (d) except in the case of any Insurances provided by an Affiliate of the Supplier, of good repute in the international insurance market.
- 1.4 The Supplier shall ensure that the public and products liability policy shall contain an indemnity to principals clause under which the Authority shall be indemnified in respect of claims made against the Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Contract and for which the Supplier is legally liable.

2 GENERAL OBLIGATIONS

- 2.1 Without limiting the other provisions of this Contract, the Supplier shall:
- (a) take or procure the taking of all reasonable risk management and risk control measures in relation to the Services as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;
 - (b) promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

SCHEDULE 6 (INSURANCE REQUIREMENTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (c) hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

3 FAILURE TO INSURE

- 3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.
- 3.2 Where the Supplier has failed to purchase any of the Insurances or maintain any of the Insurances in full force and effect, the Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances, and the Authority shall be entitled to recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4 EVIDENCE OF INSURANCES

- 4.1 The Supplier shall upon the Effective Date and within 15 Working Days after the renewal or replacement of each of the Insurances, provide evidence, in a form satisfactory to the Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule. Receipt of such evidence by the Authority shall not in itself constitute acceptance by the Authority or relieve the Supplier of any of its liabilities and obligations under this Contract.

5 CANCELLATION

- 5.1 Subject to Paragraph 6.2, the Supplier shall notify the Authority in writing at least 5 Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.
- 5.2 Without prejudice to the Supplier's obligations under Paragraph 4, Paragraph 6.1 shall not apply where the termination of any Insurances occurs purely as a result of a change of insurer in respect of any of the Insurances required to be taken out and maintained in accordance with this Schedule.

6 INSURANCE CLAIMS, PREMIUMS AND DEDUCTIBLES

- 6.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Services and/or this Contract for which it may be entitled to claim under any of the Insurances. In the event that the Authority receives a claim relating to or arising out of the Services and/or this Contract, the Supplier shall co-operate with the Authority and assist it in dealing with such claims at its own expense including without limitation providing information and documentation in a timely manner.
- 6.2 The Supplier shall maintain a register of all claims under the Insurances in connection with this Contract and shall allow the Authority to review such register at any time.

SCHEDULE 6 (INSURANCE REQUIREMENTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- 6.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.
- 6.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

SCHEDULE 6 (Insurance Requirements) – Annexes

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 1: REQUIRED INSURANCES

PART A: INSURANCE CLAIM NOTIFICATION

Except where the Authority is the claimant party, the Supplier shall give the Authority notice within 20 Working Days after any insurance claim in excess of [REDACTED] relating to or arising out of the provision of the Services or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Authority) full details of the incident giving rise to the claim.

PART B: THIRD PARTY PUBLIC AND PRODUCTS LIABILITY INSURANCE

1 Insured

1.1 The Supplier

2 Interest

2.1 To indemnify the Insured in respect of all sums which the Insured shall become legally liable to pay as damages, including claimant's costs and expenses, in respect of accidental:

- (a) death or bodily injury to or sickness, illness or disease contracted by any person; and
- (b) loss of or damage to physical property;

happening during the period of insurance (as specified in Paragraph 5) and arising out of or in connection with the provision of the Services and in connection with this Contract.

3 Limit of indemnity

3.1 Not less than [REDACTED] in respect of any one occurrence, the number of occurrences being unlimited in any annual policy period, but [REDACTED] in the aggregate per annum in respect of products and pollution liability.

4 Territorial limits

United Kingdom (or worldwide, where applicable)

5 Period of insurance

5.1 From the date of this Contract for the Term and renewable on an annual basis unless agreed otherwise by the Authority in writing.

6 Cover features and extensions

6.1 Indemnity to principals clause under which the Authority shall be indemnified in respect of claims made against the Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Contract and for which the Supplier is legally liable.

SCHEDULE 6 (Insurance Requirements) – Annexes

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

7 Principal exclusions

- 7.1 War and related perils.
- 7.2 Nuclear and radioactive risks.
- 7.3 Liability for death, illness, disease or bodily injury sustained by employees of the Insured arising out of the course of their employment.
- 7.4 Liability arising out of the use of mechanically propelled vehicles whilst required to be compulsorily insured by applicable Law in respect of such vehicles.
- 7.5 Liability in respect of predetermined penalties or liquidated damages imposed under any contract entered into by the Insured.
- 7.6 Liability arising out of technical or professional advice other than in respect of death or bodily injury to persons or damage to third party property.
- 7.7 Liability arising from the ownership, possession or use of any aircraft or marine vessel.
- 7.8 Liability arising from seepage and pollution unless caused by a sudden, unintended and unexpected occurrence.

8 Maximum deductible threshold

- 8.1 Not to exceed [REDACTED] for each and every third party property damage claim (personal injury claims to be paid in full).

PART C: UNITED KINGDOM COMPULSORY INSURANCES

The Supplier shall meet its insurance obligations under applicable Law in full, including, UK employers' liability insurance and motor third party liability insurance.

PART D: PROFESSIONAL INDEMNITY INSURANCE

1. Insured

- 1.1 The Supplier

2. Interest

- 2.1 To indemnify the Insured in respect of all sums which the Insured shall become legally liable to pay (whether contractually or otherwise) as damages, including claimant's costs and expenses, as a result of claims first made against the Insured during the Period of Insurance by reason of any negligent act, error and/or omission arising out of or in connection with the provision of professional advice and/or services in connection with this Contract.

SCHEDULE 6 (Insurance Requirements) – Annexes

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

3. Limit of indemnity

- 3.1 Not less than [REDACTED] in respect of any one claim and in the aggregate per annum.

4. Territorial limits

- 4.1 United Kingdom (or worldwide, where applicable)

5. Period of insurance

- 5.1 From the date of this Contract for the Term and renewable on an annual basis unless agreed otherwise by the Authority in writing and a period of six (6) years following the earlier of the expiry or termination of this Contract.

6. Cover features and extensions

- 6.1 In respect of any claims made policy wording, full retroactive cover or retroactive date to be no later than the date of this Contract.

7. Principal exclusions

- 7.1 War and related perils.
7.2 Nuclear and radioactive risks.

SCHEDULE 7 (Authority Responsibilities)
Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SCHEDULE 7

AUTHORITY RESPONSIBILITIES

SCHEDULE 7 (Authority Responsibilities)
Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Schedule 7 (*Authority Responsibilities*)

1 INTRODUCTION

- 1.1 The responsibilities of the Authority set out in this Schedule shall constitute the Authority Responsibilities under this Contract. Any obligations of the Authority in Schedule 2 (Services Description) and Schedule 8 (Supplier Solution) shall not be Authority Responsibilities and the Authority shall have no obligation to perform any such obligations unless they are specifically stated to be "Authority Responsibilities" and cross referenced in the table in Paragraph 3.
- 1.2 The responsibilities specified within this Schedule shall be provided to the Supplier free of charge, unless otherwise agreed between the Parties.

2 GENERAL OBLIGATIONS

- 2.1 The Authority shall:
- a) perform those obligations of the Authority which are set out in the Clauses of this Contract, the Paragraphs of the Schedules (except Schedule 2 (Services Description) and Schedule 8 (Supplier Solution)) and in the 'Authority Responsibilities (if applicable)' column of the table in Annex 1 (Outline Implementation Plan) to Schedule 13 (Implementation Plan) or as replaced in the approved Detailed Implementation Plan in accordance with Paragraph 3.6 of Schedule 13;
 - b) use its reasonable endeavours to provide the Supplier with access to appropriate members of the Authority's staff, as such access is reasonably requested by the Supplier in order for the Supplier to discharge its obligations throughout the Term and the Termination Assistance Period;
 - c) provide sufficient and suitably qualified staff to fulfil the Authority's roles and duties under this Contract as defined in the Implementation Plan;
 - d) use its reasonable endeavours to provide such documentation, data and/or other information that the Supplier reasonably requests that is necessary to perform its obligations under the terms of this Contract provided that such documentation, data and/or information is available to the Authority and is authorised for release by the Authority; and
 - e) procure for the Supplier such agreed access and use of the Authority Premises (as a licensee only) and facilities (including relevant IT systems) as is reasonably required for the Supplier to comply with its obligations under this Contract, such access to be

provided during the Authority's normal working hours on each Working Day or as otherwise agreed by the Authority (such agreement not to be unreasonably withheld or delayed).

3 SPECIFIC OBLIGATIONS

3.1 The Authority shall, in relation to this Contract perform the Authority's responsibilities identified as such in this Contract the details of which are set out below:

Table 1: Authority Responsibilities

ID	Relevant Document	Authority Responsibility
AO-001	Technical Requirements	The Authority shall be responsible for the Civil Works and Remediation required within the boundary of an Authority Site, to enable the Services to be received within the boundary of that Authority Site. For the avoidance of doubt, the Supplier shall be responsible for all Civil Works and Remediation outside the boundary of the Authority Site.
AO-002	Service Management Requirements	The Authority shall provide and maintain the ITSM Toolset as is reasonably required to: a) allow the Supplier to establish connection for the exchange of near real-time data and/or to access and utilise it; and b) ensure availability of and access to the ITSM Toolset and the supporting configurations and data sets to a reasonable number of authorised Supplier users and, where relevant, via the [REDACTED]. Note that the Authority's responsibilities do not include the maintenance of any integration with a Supplier-owned ITSM toolset.
AO-003	Technical Requirements	The Authority shall provide and manage the [REDACTED]
AO-004	Technical Requirements	The Authority shall provide the Supplier with the necessary configuration information to connect to the Authority's DNS service and shall update and maintain the required National Cyber Security Centre protective DNS service entries to enable the Supplier to integrate / interface the Operational Services with

SCHEDULE 7 (Authority Responsibilities)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ID	Relevant Document	Authority Responsibility
		the Authority's DNS services (see requirements 3.2.3.2 and 4.4.2.1 in the Technical Requirements).
AO-005	Technical Requirements	The Authority shall provide the Supplier with read access to the required DHCP scopes to enable the Supplier to interface with the Authority's DHCP service (see requirement 4.6.1.10 in the Technical Requirements).
AO-006	Technical Requirements	The Authority shall procure PSN access to enable ViSOR access in accordance with requirement 3.4.2.1 of the Technical Requirements.
AO-007	Technical Requirements	Unless the IPAM Service has been implemented under the Contract, the Authority shall provide IPAM and shall provide access to its IPAM toolset for sufficient Supplier Personnel to enable the Supplier to interface with the IPAM toolset in accordance with requirement 4.4.1.1 of the Technical Requirements.
AO-009	Paragraphs 2.2.1 and 2.3.5 of the Technical Requirements and Paragraph 7.2 of the Transition Requirements	Where requested in advance in writing by the Supplier for installation of Devices at Authority Site(s), the Authority shall purchase and arrange for delivery to the Supplier the following products in accordance with the process agreed between the Parties from time to time for the supply of such products: a) SD-WAN Edge Devices; b) interface cards for SD-WAN Edge Devices; c) rackmount kits for SD-WAN Edge Devices; d) intelligent power strips; and e) SIM cards, for mobile broadband Services as described in Paragraph 2.3.5 of the Technical Requirements.
AO-010	Service Management Requirements	The Authority shall provide the Authority's Service Desk which shall be responsible for dealing with End Users where they relate to Incidents, compliments, complaints or escalations, and shall:

SCHEDULE 7 (Authority Responsibilities)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ID	Relevant Document	Authority Responsibility
		a) liaise with appropriately trained and skilled expert resource from the Supplier as required to handle the End User's query; b) handle End User queries to the extent provided for in the relevant information received from the Supplier. For the sake of clarity, the Supplier is responsible for contacting End Users for troubleshooting and Incident resolution where appropriate and the Authority is responsible for informational communications; c) manage progress of Incidents through the Incident lifecycle utilising the Supplier updates recorded in the ITSM Toolset, and update the End User on progress; and d) update End Users in a timely and accurate manner with any updates recorded in the ITSM Toolset.
AO-011	Technical Requirements	Where, following a site survey, the Supplier notifies the Authority that an Authority Site requires additional works (e.g. power and rack space) to meet the standards of feasibility and readiness required for installation and operation of required Devices, the Authority shall be responsible for conducting such works as it determines will be required prior to requiring deployment of the relevant Device(s).
AO-012	Prison Service Instructions (as referenced in Schedule 4 (<i>Standards</i>))	a) The Authority shall provide the Supplier with the form of authorisation required for requesting use, conveyance and possession of tools and/or other controlled items in prisons, as required for delivery of the Services ("Tool List"). b) The Authority shall coordinate with the prisons the Supplier's requests for authorisation of Tool Lists.
AO-013	Technical Requirements	The Authority shall use reasonable endeavours to obtain consents and wayleaves required by the Supplier for the provision of the Services where: a) such consents and/or wayleaves relate to an Authority Site; and b) such consents or wayleaves can only be obtained from the landlord and/or agents

SCHEDULE 7 (Authority Responsibilities)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ID	Relevant Document	Authority Responsibility
		(including building management and solicitors) of that Authority Site; and c) the requirement for such consent or wayleave to be obtained by the Authority is clearly set out in the Implementation Plan or a Project Plan. The Authority shall notify the Supplier when wayleaves/consents have been obtained and/or any delays or problems with obtaining the wayleave/consent and shall allow the Supplier reasonable sufficient time (as determined by the Authority acting reasonably) to reschedule the relevant works following such notification and/or to accommodate any such delay or problem.
AO-014	Technical Requirements and Transition Requirements	Where Authority Site access has been requested by the Supplier in accordance with the Authority Site Access Request Process, the Authority shall: a) support completion of necessary documentation in order to gain access; and b) manage the co-ordination with personnel at the Authority Site to arrange dates, times and named site contacts for visits.
AO-015	Technical Requirements and Transition Requirements	Where the Authority Representative becomes aware of any change within an Authority Comms Room subsequent to a Site readiness survey conducted by the Supplier, and where such change will prevent the Supplier from undertaking works for delivery of Services, the Authority shall: a) request an Operational Change or Change; and/or b) conduct such Remediation as is necessary (if any) to enable the relevant works to be completed. The Authority shall notify the Supplier of the completion date for such Remediation and shall allow the Supplier sufficient time (as determined by the Authority acting reasonably) to reschedule the relevant works following such notification.
AO-016	Service Management Requirements (Paragraph 6.3.2.6)	Each month following delivery by the Supplier of the Capacity Report, the Authority shall review the Capacity Report and where utilisation at an Authority Site is reasonably forecast to exceed the Target Performance Levels of the Capacity Management KPI

SCHEDULE 7 (Authority Responsibilities)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ID	Relevant Document	Authority Responsibility
	and “Capacity Management” KPI as set out in Schedule 3 (<i>Performance Levels</i>)	and the Supplier has recommended specific reasonable mitigating action, the Authority shall: a) either submit a Request for additional capacity at the relevant Authority Site; or b) use reasonable endeavours to manage the relevant Access Circuit utilisation at the relevant Authority Site within the CDR specified in the Authority Site Specification.
AO-017	Baseline Security Requirements (Paragraph 10.7, Annex 1 to Schedule 5 (Security Management Requirements))	The Authority shall provide network connectivity from the boundary of the management access layer of the Gateway System to its cybersecurity log platform, syslog collector and VM broker.
AO-018	Service Management Requirements	The Authority shall ensure that the ITSM Toolset has the level of functionality and features required by the Authority to enable the Authority and/or the Supplier (as the case may be) to: a) record information for the following Processes: • Demand Management; • Service Portfolio Management; • Service Asset and Configuration Management; • Product and Service Catalogue Management; • Service Level Management; • Change and Evaluation Management; • Transition Planning and Support; • Release and Deployment Management; • Licence Management and Compliance; and • Continual Service Improvement; b) maintain the Product & Service Catalogue, including to describe Catalogue Items; c) progress Service Requests; d) make written records of: • communications with End Users;

SCHEDULE 7 (Authority Responsibilities)
Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ID	Relevant Document	Authority Responsibility
		analysis, investigations and recovery actions that have been taken to resolve an Incident; and e) raise and progress Service Changes.

3.2 Where the Optional Services listed in Table 2 have been implemented pursuant to Clause 5.10, the Authority shall, in relation to such Optional Services perform the Authority's responsibilities identified as such in Table 2:

Table 2: Authority Responsibilities (Optional Services)

ID	Relevant Document	Optional Service	Authority Responsibility
AO-102	Service Management Requirements	SASE Services (Optional Service)	The Authority shall ensure that the Other Supplier(s) of support services subscriptions for SD-WAN Edge Devices will accept agency management as required to support Paragraph 6.8.5 of the Service Management Requirements.

SCHEDULE 8 (SUPPLIER SOLUTION)
Confidential
Contract for the provision of WAN Services

Security Classific [REDACTED] al)
Contract referenc [REDACTED]

SCHEDULE 8

SUPPLIER SOLUTION

Schedule 8 (*Supplier Solution*)

1 Definitions

1.1 In this Schedule, unless the context otherwise requires, capitalised expressions shall have the meanings set out in Schedule 1 (Definitions). Furthermore, the following definition shall apply:

“Tender” means the offer including all supporting tender response documents, rates and prices and proposals which was submitted by the Supplier in response to the invitation to submit final tenders document issued by the Authority for the procurement of the Services.

2 Background and introduction

2.1 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.6 The solutions for the Technical Requirements, Service Management Requirements and Transition Requirements are addressed respectively by:

2.6.1 Annex A (Technical Solution);

2.6.2 Annex B (Service Management Solution); and

2.6.3 Annex C (Transition Solution).

2.7 Annex D (Resource Profile) sets out the Supplier’s anticipated resourcing arrangements to deliver the Services. Note that the social value requirements of Annex D to the Services Description will be delivered in accordance with the Social Value Delivery Plan.

SCHEDULE 8 (SUPPLIER SOLUTION)
Confidential
Contract for the provision of WAN Services

Security Classific[REDACTED]al)
Contract referenc[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION)

Confidential

Contract for the provision of WAN Services

Security Classific [REDACTED] al)

Contract reference

© 2006 The Authors
Journal compilation © 2006 Blackwell Publishing Ltd

[REDACTED]

[REDACTED]

4 Summary

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION)
Confidential
Contract for the provision of WAN Services

Security Classific[REDACTED]al)
Contract referenc[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION)
Confidential
Contract for the provision of WAN Services

Security Classific[REDACTED]al)
Contract referenc[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION)
Confidential
Contract for the provision of WAN Services

Security Classification [REDACTED] al)
Contract reference [REDACTED]

■	[REDACTED]
[REDACTED]	
[REDACTED]	
[REDACTED]	
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
[REDACTED]	
[REDACTED]	
[REDACTED]	
■	[REDACTED]
[REDACTED]	

SCHEDULE 8 (SUPPLIER SOLUTION)
Confidential
Contract for the provision of WAN Services

Security Classific[REDACTED]al)
Contract referenc[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION)

Confidential

Contract for the provision of WAN Services

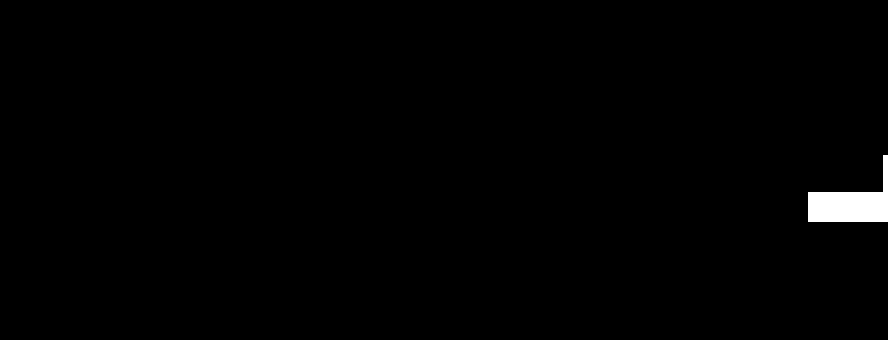
Security Classific [REDACTED] al)

Contract reference [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION)
Confidential
Contract for the provision of WAN Services

Security Classific[REDACTED]al)
Contract referenc[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION)
Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION)
Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION)
Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION)
Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION)
Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION)
Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION)
Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 8

(Supplier Solution)

Annex A – Technical Solution

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Introduction

This Annex A (Technical Solution) to Schedule 8 (Supplier Solution) sets out the Supplier's technical solution to ensure that the Supplier meets the Technical Requirements. It contains the following sections:

- 3.1 Field Services;
- 3.2 WAN Connectivity: Transport Services;
- 3.4 Gateway Services;
- 3.5 Core Network Services; and
- 3.6 Scalability and Flexibility.

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]	
[REDACTED]	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
[REDACTED]	

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED]	

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference:

	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX A (TECHNICAL SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Schedule 8
(Supplier Solution)

Annex B – Service Management Solution

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Introduction

This Annex B (Service Management Solution) to Schedule 8 (Supplier Solution) sets out the Supplier's service management solution to ensure that the Supplier meets the Service Management Requirements. It contains the following sections:

- 2.1 Service Management;
- 2.2 Service Levels and Performance Monitoring;
- 2.3 Approach to in-life requests;
- 2.4 Other WAN Supplier management and Connectivity Services;
- 2.5 Continual Service Improvement; and
- 2.6 Security Management (Performance Indicators).

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]		[REDACTED]		[REDACTED]		[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]				
		[REDACTED]	[REDACTED]				
		[REDACTED]					

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]		[REDACTED]		[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		
		[REDACTED]	[REDACTED]		
[REDACTED]		[REDACTED]			

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

■ [REDACTED]

■ [REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX B (SERVICE MANAGEMENT SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 8

(Supplier Solution)

Annex C – Transition Solution

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Introduction

This Annex C (Transition Solution) to Schedule 8 (Supplier Solution) sets out the Supplier's Solution to ensure that the Supplier meets the Transition Requirements. It contains the following sections:

- 4.1 Service Continuity;
- 4.2 Implementation Plan;
- 4.3 Transition - Approach;
- 4.4 Transition – Operating Model, People and Team; and
- 4.5 Transition – Third party management.

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

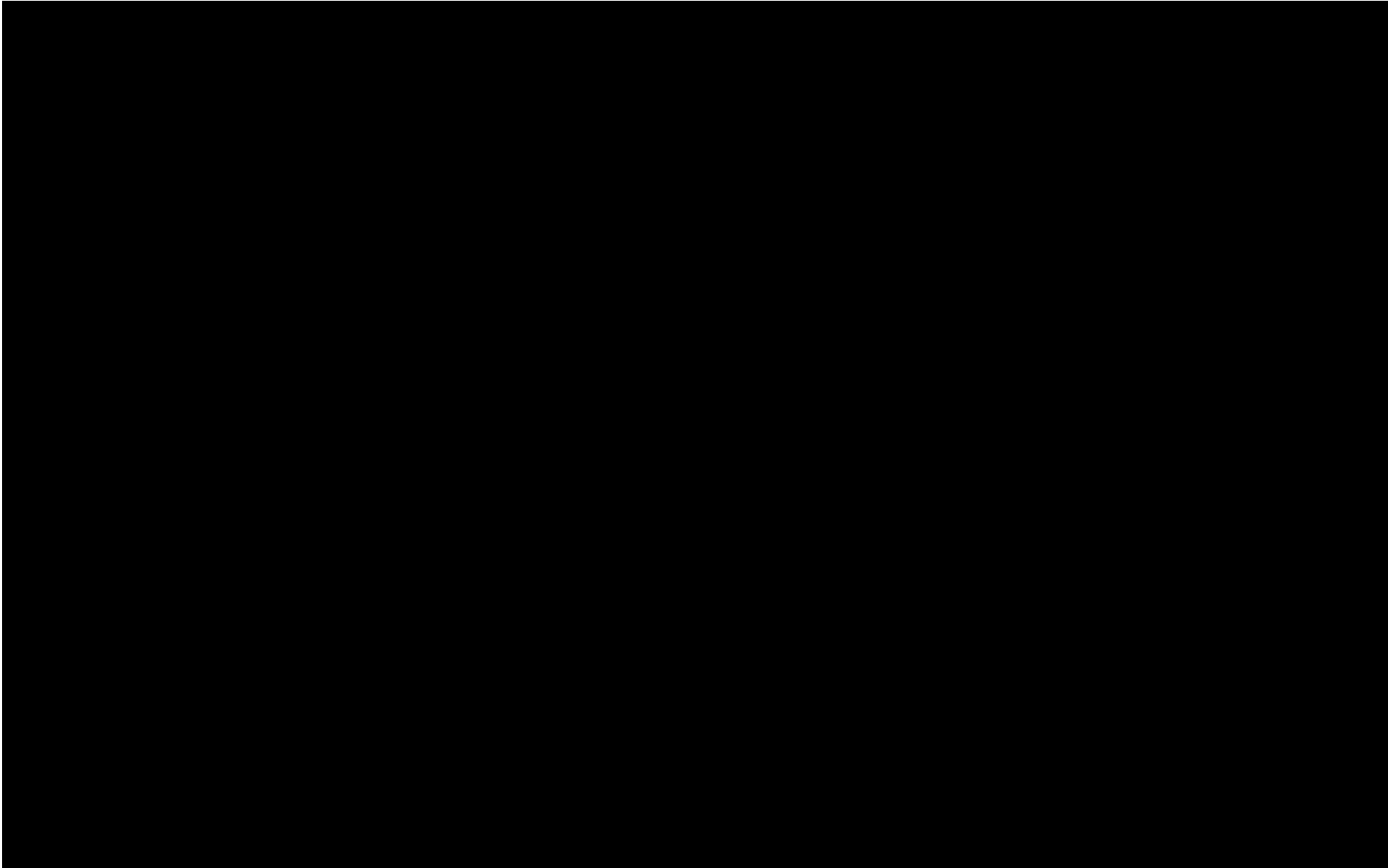
SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]



SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Secuirty Classification (Official)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference:

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Table 2: Milestone planned completion dates

[REDACTED]		[REDACTED]		[REDACTED]	
[REDACTED]		[REDACTED]		[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference:

1. **Introduction**

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

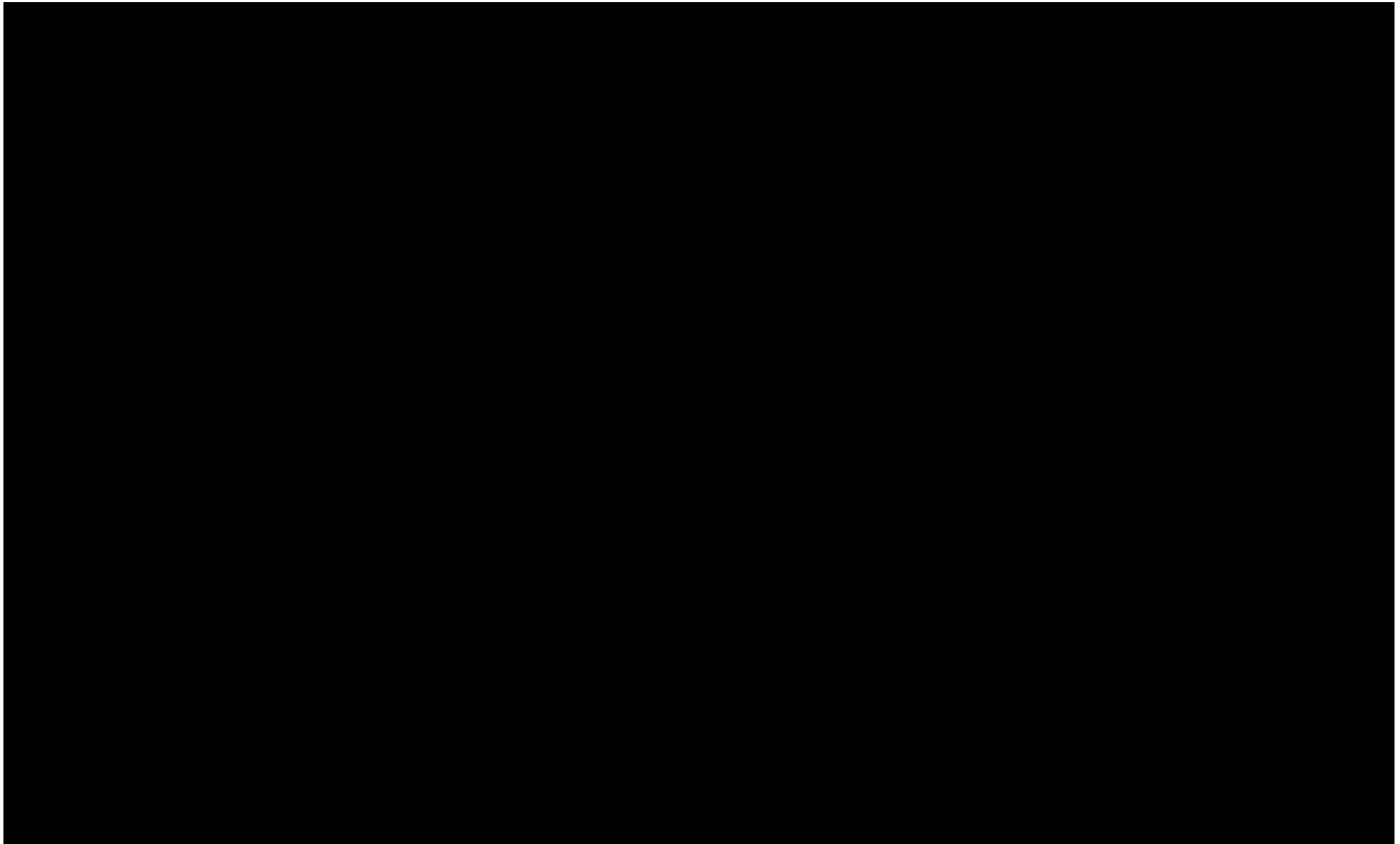
[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Secuirty Classification (Official)

Confidential [REDACTED]

Contract for the provision of WAN Services



SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Security Classification (Official)

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Secuirty Classification (Official)

Confidential
Contract for the provision of WAN Services

[Redacted]

[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

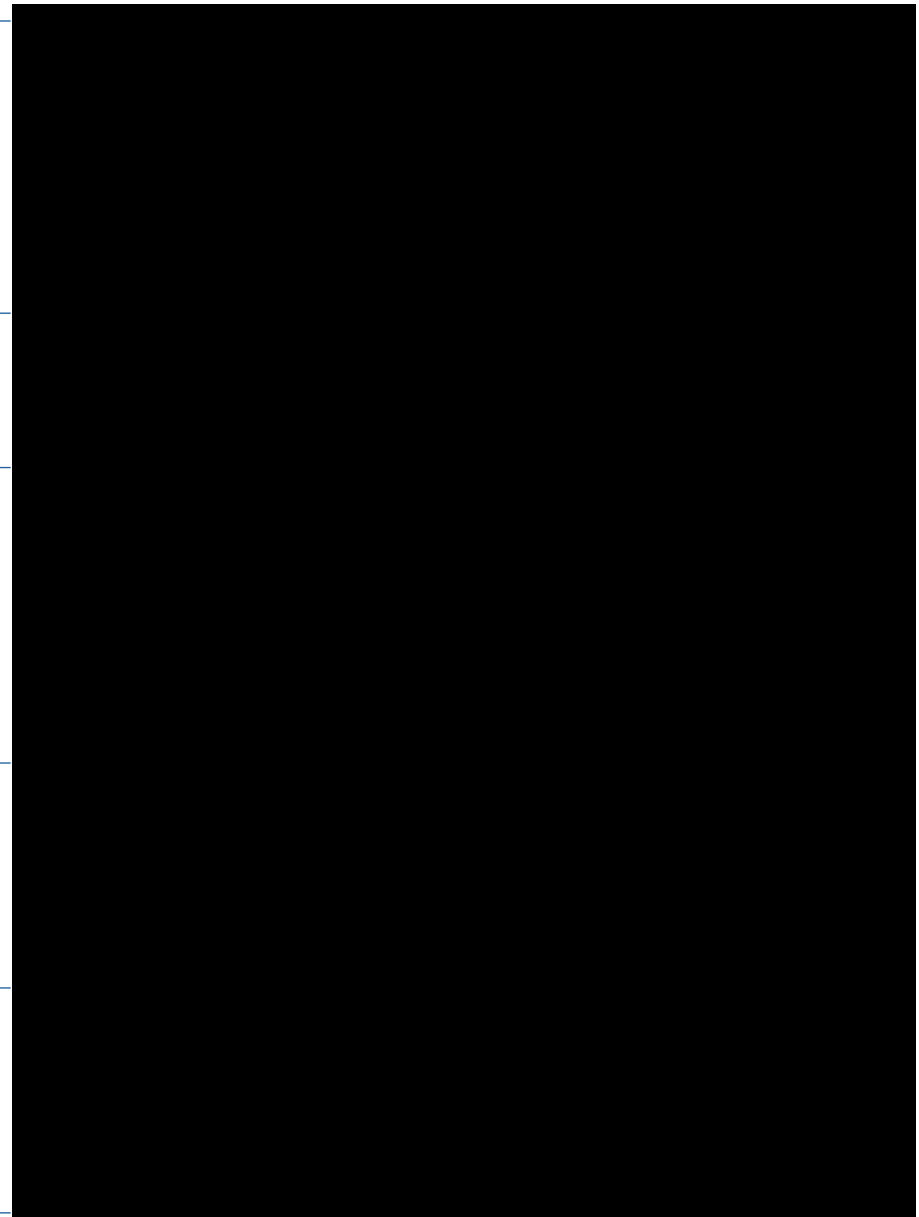
Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]



SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Security Classification (Official)

Confidential
Contract for the provision of WAN Services

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Contract for the provision of WAN Services

1000

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

- [Redacted]
- [Redacted]

[Redacted]

- [Redacted]

[Redacted]

[Redacted]

[Redacted]	[Redacted]
[Redacted]	[Redacted] [Redacted]
[Redacted]	[Redacted]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Security Classification (Official)

Confidential
Contract for the provision of WAN Services

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

[REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

[REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

	[REDACTED] [REDACTED] [REDACTED] [REDACTED]	
[REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

	[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference:

	[REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

	[REDACTED] [REDACTED]	

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Security Classification (Official)
[REDACTED]

Confidential
Contract for the provision of WAN Services

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20
21	22	23	24
25	26	27	28
29	30	31	32
33	34	35	36
37	38	39	40
41	42	43	44
45	46	47	48
49	50	51	52
53	54	55	56
57	58	59	60
61	62	63	64
65	66	67	68
69	70	71	72
73	74	75	76
77	78	79	80
81	82	83	84
85	86	87	88
89	90	91	92
93	94	95	96
97	98	99	100

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	[REDACTED]		
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]		[REDACTED]
[REDACTED]	[REDACTED]		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]		[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]	
[REDACTED]		[REDACTED]	

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX C (TRANSITION SOLUTION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 8

(Supplier Solution)

Annex D – Resource Profile

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Introduction

This Annex D (Resource Profile) to Schedule 8 (Supplier Solution) sets out the Supplier's resource profile to deliver the Operational Services and Transition and the Supplier's approach to recruitment, training, onboarding and personnel development to meet the Authority Requirements. It contains the following sections:

- Outline of the Supplier's resource model to deliver the Operational Services;
- Indicative resource profile to be utilised in the planned delivery of the Relevant Authority Requirements;
- People and team – the Supplier's approach to recruitment, training, onboarding and personnel development; and
- The operating and resource models for Transition.

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference:

[illegible]

[REDACTED]

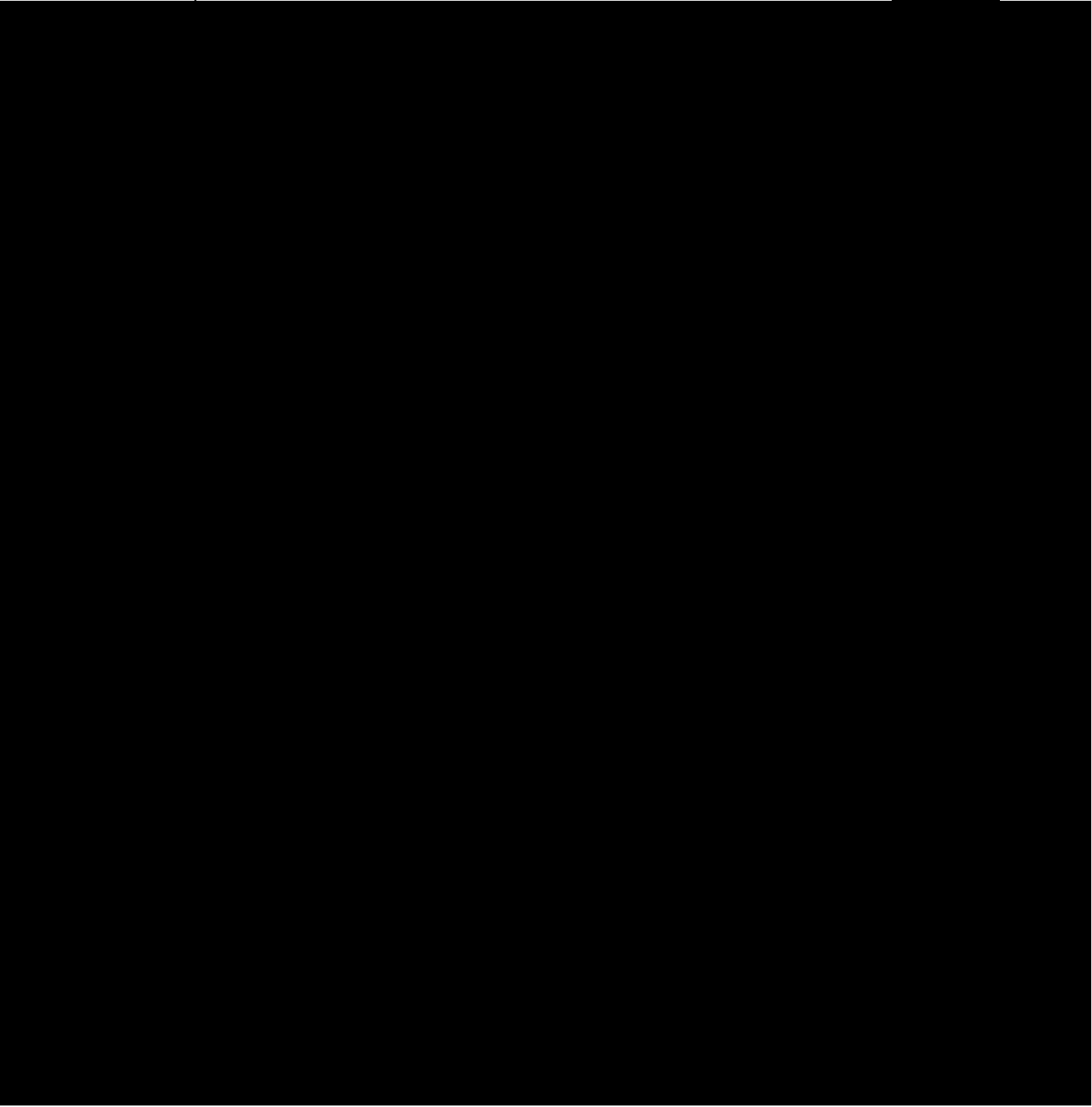
SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]



SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]	[REDACTED]
	[REDACTED]
[REDACTED]	

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]	[REDACTED]
	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

[illegible]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]	[REDACTED]
	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

[illegible]

1. [REDACTED]
 2. [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

[illegible]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]	[REDACTED]
	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]	[REDACTED]
	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]		[REDACTED]		[REDACTED]		[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]				
	[REDACTED]	[REDACTED]	[REDACTED]				
	[REDACTED]	[REDACTED]	[REDACTED]				
	[REDACTED]	[REDACTED]	[REDACTED]				
	[REDACTED]	[REDACTED]	[REDACTED]				
[REDACTED]		[REDACTED]					

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- [REDACTED]
- [REDACTED]

[REDACTED]

SCHEDULE 8 (SUPPLIER SOLUTION) - ANNEX D (RESOURCE PROFILE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 9 (COMMERCIALLY SENSITIVE INFORMATION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 9

COMMERCIALLY SENSITIVE INFORMATION

SCHEDULE 9 (COMMERCIALLY SENSITIVE INFORMATION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 9 (Commercially Sensitive Information)

- 1 In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.
- 2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below (please see the column "Duration of Confidentiality").
- 3 Without prejudice to the Authority's obligation to disclose Information in accordance with FOIA or Clause 19 (Confidentiality), the Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

Commercially Sensitive Information

No.	Date	Item(s)	Duration of Confidentiality
1	Date of Submission	The Supplier's charges including tender responses, rate cards and any volume and utilisation discounts provided.	Term plus 6 years
2	Date of Submission	Breakdown of pricing information to give input costs, capital and operating costs, overheads, revenue, margins and profits.	Term plus 6 years
3	Date of Submission	How any payments due to the Supplier on termination of the whole or any part of the Agreement have been or will be calculated but excluding the actual amounts of such payments.	Term plus 6 years
4	Date of Submission	Any financial data relating to the Supplier's business as a whole including the financial standing of the Supplier provided in connection with this Agreement, including but not limited to any information relating to financial distress reporting.	Term plus 6 years
5	Date of Submission	Liability and indemnities; including the amount of any caps, any unlimited heads of losses and any excluded heads of losses.	Term plus 6 years

SCHEDULE 9 (COMMERCIALLY SENSITIVE INFORMATION)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

6	Date of Submission	The cover and amounts of the Supplier's insurances.	Term plus 6 years
7	Date of Submission	How any Service Credits are financially calculated under the Agreement, but excluding the details regarding the applicable service thresholds, or any performance related information or requirements, or information relating to the actual amounts of any Service Credits paid or credited to the Buyer.	Term plus 6 years
8	Date of Submission	Technical details of the Supplier's network (including topology, network diagrams, detailed network coverage, route maps, The Supplier's Points of Presence and/or street furniture/chambers etc.)	Term plus 6 years
9	Date of Submission	Design documents relating to the Services and any notes or minutes of technical design meetings held in relation to the aforementioned but excluding any documents set out in the Agreement as being Deliverables to the Buyer.	Term plus 6 years
10	Date of Submission	Any Supplier proposals in response to Variations to the extent that the information falls within one of the other items set out in this table and innovation proposals provided under the Agreement including in a response to a Variation.	Term plus 6 years
11	Date of Submission	Staff information generally including personal details	Term plus 6 years
12	Date of Submission	The Supplier's own Business Continuity and Disaster Recovery Plan (including any Business Incident Plans, Disaster Recovery Manuals and Procedures, Security Plan and Related Business Security Processes) but excluding any Buyer specific plans or procedures to be provided by the Supplier under the Agreement.	Term plus 6 years

SCHEDULE 10 (NOTIFIED KEY SUB-CONTRACTORS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 10

NOTIFIED KEY SUB-CONTRACTORS

SCHEDULE 10 (NOTIFIED KEY SUB-CONTRACTORS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Schedule 10 (*Notified Key Sub-Contractors*)

- 1 In accordance with Clause 15.11 (*Appointment of Key Sub-contractors*), the Supplier is entitled to sub-contract its obligations under this Contract to the Key Sub-contractors listed in the table below.
- 2 The Parties agree that they will update this Schedule periodically to record any Key Sub-contractors appointed by the Supplier with the consent of the Authority after the Effective Date for the purposes of the delivery of the Services.

Key Sub-contractor name and address (if not the same as the registered office)	Registered office and company number	Related product/Service description	Key Sub-contract price expressed as a percentage of total projected Charges over the Term	Key role in delivery of the Services	Credit Rating Threshold

[REDACTED]					

SCHEDULE 11 (THIRD PARTY CONTRACTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 11

THIRD PARTY CONTRACTS

SCHEDULE 11 (THIRD PARTY CONTRACTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Schedule 11 (*Third Party Contracts*)

PART A: Third Party Contracts

- 1 The contracts listed in the table below constitute Third Party Contracts entered into exclusively for the purposes of delivering the Services.
- 2 The Supplier shall be entitled to update this Schedule in accordance with Clause 15.5 (*Appointment of Sub-contractors*).

Third party supplier name and address (if not the same as the registered office)	Registered office and company number	Related product/service description
[REDACTED]	[REDACTED]	[REDACTED]

SCHEDULE 11 (THIRD PARTY CONTRACTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

PART B: Transferring Agreements

The following table provides a list of Transferring Agreements. The Authority will liaise with the Supplier once it has identified a Transferring Agreement and the effect of any Change necessitated by the transfer of responsibility for services and equipment within the scope of the Transferring Agreement will be agreed in accordance with the Change Control Procedure as set out in Clause 9.8 (Transferring Agreements).

Third party supplier name, company number and registered office	Agreement Description	Relevant Agreed Transfer Date

SCHEDULE 11 (THIRD PARTY CONTRACTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Template Managed Agency Agreement referred to in Clause 9.9 (Transferring Agreements)

TEMPLATE MANAGED AGENCY AGREEMENT

[On Authority Headed Paper]

[Authority Address]

[YY Name

and Address]

Dear [YY],

RE: Managed Agency Agreement

Background

- (A) The Secretary of State for Justice ("**Ministry of Justice**") has recently entered into an outsourcing arrangement whereby [REDACTED] (company registration number [REDACTED]) whose registered office is at [REDACTED] ("**XX**") will provide to the Ministry of Justice WAN services, as defined in the contract for the provision of WAN Services dated [xxx] 20[] (the "**WAN Contract**").
- (B) Pursuant to the [name of agreement] dated [date of agreement] [as amended from time to time by Contract Change Notes ("**CCN**") between [insert name of YYYY] (company registration number [REDACTED]) with registered address at [insert address of YY] ("**YY**") and the Ministry of Justice (the "**Applicable Contract**"), YY provides (amongst other things) the following services to the Ministry of Justice: [set out the relevant services] ("**the Applicable Services**").
- (C) YY, XX and the Ministry of Justice shall collectively be known as "**the Parties**".
- (D) It has been agreed by the Parties that XX shall act as the Ministry of Justice's agent with respect to the Applicable Services on the terms of this agreement ("**Letter of Agency**") to enable XX to manage the Applicable Services on the Ministry of Justice's behalf.

In this context, the Parties have entered into this Letter of Agency to set out the terms of the agency arrangement between the Parties. Accordingly, in consideration of the sum of [REDACTED], the receipt and sufficiency of which YY hereby acknowledges, the Parties agree to the terms of this Letter of Agency as set out below.

SCHEDULE 11 (THIRD PARTY CONTRACTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Terms and Conditions

1. The Ministry of Justice hereby appoints XX to act as its agent to carry out the management of the Applicable Services under the Applicable Contract (the “**Agency Services**”) on the terms of this Letter of Agency and XX accepts the appointment on these terms.
2. In order for XX to transition and maintain a live network for the Ministry of Justice and facilitate a staged de-commissioning of the Applicable Services provided by YY under the Applicable Contract, the Ministry of Justice hereby appoints XX to act as agent on behalf of Ministry of Justice in relation to the Applicable Services under the Applicable Contract in respect of the matters set out in the Annex to this Letter of Agency only:
3. Save as set out in paragraph 2 above and the Annex, in all other respects, YY and the Ministry of Justice shall remain bound by the Applicable Contract. For the avoidance of doubt, except as set out in paragraph 2 above and the Annex, the contractual management and payment obligations and responsibilities shall remain as set out in the Applicable Contract between [YY] and the Ministry of Justice.
4. XX and YY shall ensure that the day to day operation of the Applicable Services under the Applicable Contract shall not be affected by this Letter of Agency, except as agreed as part of the exit obligations on YY under **[insert relevant provision cross-reference]** of the Applicable Contract and transition obligations on XX under Schedule 2 (Services Description) and Schedule 13 (Implementation Plan) of the WAN Contract.
5. YY and XX shall work together to minimise any disruption to the Applicable Services as a result of this Letter of Agency.
6. YY shall use its reasonable endeavours to ensure that there shall be no break or deterioration in the Applicable Services as a result of this Letter of Agency.
7. XX shall (subject to receiving the Applicable Contract from YY pursuant to paragraph 9 below), use its reasonable endeavours to ensure that there shall be no break or deterioration in the Applicable Services as a result of this Letter of Agency.
8. In respect of the Agency Services, XX shall:
 - (a) act conscientiously and in good faith and not allow its interests to conflict with the duties that it owes the Ministry of Justice under this Letter of Agency, the WAN Contract and under general law;

SCHEDULE 11 (THIRD PARTY CONTRACTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (b) except as authorised by the Ministry of Justice in writing, not act in a way which will incur any liabilities on behalf of the Ministry of Justice nor to pledge the credit of the Ministry of Justice;
- (c) comply with all reasonable and lawful instructions of the Ministry of Justice from time to time concerning the Agency Services;
- (d) not take part in any dispute or commence or defend any court or other dispute proceedings or settle or attempt to settle or make any admission concerning such proceedings;
- (e) not cause the Ministry of Justice to be in breach of the Applicable Contract, (subject to XX receiving the Applicable Contract from YY pursuant to paragraph 9 below) or any other applicable law when acting as the Ministry of Justice's agent in respect of the Agency Services;
- (f) indemnify the Ministry of Justice against any liabilities (including reasonable legal fees) which are incurred by or awarded against the Ministry of Justice arising from or in connection with XX's breach, negligence or non-performance of this Letter of Agency provided that the Ministry of Justice shall use all reasonable endeavours to mitigate any such losses and any such losses shall not exceed any limitations on liability set out in Clause 23 (Limitations on Liability) of the WAN Contract;
- (g) save to the extent expressly provided hereunder, not make any claim against the Ministry of Justice and/or YY in respect of any claims or liabilities arising against XX from or in connection with this Letter of Agency. XX shall be solely responsible for any associated costs and shall not be entitled to recover any additional costs or Charges from the Ministry of Justice relating to the negotiation, preparation and execution of this Letter of Agency.
- (h) abide by equivalent obligations of confidentiality to those of the Ministry of Justice within Clause [insert relevant provision cross-reference] of the Applicable Contract to keep YY's confidential information confidential (following receipt of a copy of such obligations) [and to abide by the terms of the Non-Disclosure Agreement signed between XX and YY dated [xx]];
- (i) not assign, transfer, charge or deal in any other matter with their appointment as agent with respect to the Applicable Contract or its rights under such appointment or purport to do any of the same, nor sub-contract nor appoint sub-agents or delegates of any or all of its obligations relating to such appointment;

SCHEDULE 11 (THIRD PARTY CONTRACTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- (j) not be empowered to extend, amend, renegotiate, terminate or novate the Applicable Contract (or any part thereof or subcontract thereunder) or to serve any contractual notices under the Applicable Contract unless agreed in writing by YY and the Ministry of Justice; and
 - (k) carry out the Agency Services in a manner which is consistent with its obligations under the WAN Contract.
- 9. YY will grant XX access to the Applicable Contract (including CCNs) and any other appropriate agreed documentation, currently available to the Ministry of Justice that XX may reasonably require following consultation with the Ministry of Justice to the extent necessary to enable XX to carry out the Agency Services as provided for under this Letter of Agency.
- 10. By signature of this Letter of Agency, the Ministry of Justice confirms that, at the date of this Letter of Agency, the Applicable Services delivered by YY under the Applicable Contract are free from any material defect and are in line with the agreed service levels.
- 11. Subject to the terms of this Letter of Agency, the Applicable Contract and the WAN Contract shall remain valid and in full force and effect.
- 12. This Letter of Agency shall be effective on [xx] and shall remain in effect until it terminates under paragraph 13 below.
- 13. This Letter of Agency shall automatically terminate on the earlier of:
 - (a) termination of the Applicable Contract in respect of the Applicable Services (in which case any payments on termination due to the YY or Ministry of Justice shall be governed by the terms of the Applicable Contract);
 - (b) termination of the WAN Contract;
 - (c) material breach by any of the Parties of their obligations under this Letter of Agency; or
 - (d) mutual agreement by the Parties.
- 14. Following the expiry or earlier termination of this Letter of Agency under paragraph 13 above, XX shall cease to act as agent for Ministry of Justice and shall cease to perform the Agency Services.
- 15. YY shall be responsible for its costs in the negotiation, preparation and execution of this Letter of Agency.

SCHEDULE 11 (THIRD PARTY CONTRACTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

16. This Letter of Agency and any non-contractual obligations arising out of or in connection with it will be governed by and subject to the laws of England and Wales and the parties submit to the exclusive jurisdiction of the courts of England and Wales.
17. The Parties are independent contracting parties, and nothing in this Letter of Agency shall create, or be construed as creating, any joint venture, partnership or similar arrangement between the parties.
18. The Parties may modify the Letter of Agency only if the Parties agree to do so in writing. No variation of this Letter of Agency shall be valid unless it is in writing and signed by or on behalf of each of the Parties to this Agreement.
19. A person who is not a party to this Letter of Agency shall have no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Letter of Agency provided that this shall not affect any right or remedy which exists or is available apart from that Act.

SCHEDULE 11 (THIRD PARTY CONTRACTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Annex

In accordance with paragraph 2 above, the Ministry of Justice hereby appoints XX to act as agent on behalf of Ministry of Justice in relation to the Applicable Services under the Applicable Contract in respect of the following matters only:

- (a) [XX shall manage the provision of the Applicable Services, as necessary];
- (b) [subject to any express provision in this Letter of Agency to the contrary, XX shall be permitted to instruct YY in relation to the Applicable Services];
- (c) [*list applicable matters*].

SCHEDULE 11 (THIRD PARTY CONTRACTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

We would request that you confirm receipt of this notification and your consent to the requests contained herein by signing below and returning this Letter of Agency:

Signed by the duly authorised representative of **Ministry of Justice**

Signature

Name

Title

Date

Signed by the duly authorised representative of **XX Limited**

Signature

Name

Title

Date

Signed by the duly authorised representative of **[YY]**

Signature

Name

Title

Date

SCHEDULE 12 (SOFTWARE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 12

SOFTWARE

SCHEDULE 12 (SOFTWARE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 12 (Software)

1 THE SOFTWARE

- 1.1 The Software below is licensed to the Authority in accordance with Clause 16 (*Intellectual Property Rights*) and **Schedule 32 (*Intellectual Property Rights*)**.
- 1.2 The Parties agree that they will update this Schedule regularly, and in any event no less than every 6 (six) Months from the Effective Date, to record any Supplier Software or Third Party Software subsequently licensed by the Supplier or third parties for the purposes of the delivery of the Services.

SCHEDULE 12 (SOFTWARE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

2 SUPPLIER SOFTWARE

The Supplier Software includes the following items:

Software	Supplier (if an Affiliate of the Supplier)	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/Expiry
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

3 THIRD PARTY SOFTWARE

The Third Party Software shall include the following items:

Third Party Software	Supplier	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/Expiry
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

SCHEDULE 12 (SOFTWARE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Third Party Software	Supplier	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/Expiry
				[REDACTED]			
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

SCHEDULE 12 (SOFTWARE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

SCHEDULE 12 (SOFTWARE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 1: FORM OF CONFIDENTIALITY UNDERTAKING

CONFIDENTIALITY AGREEMENT

THIS AGREEMENT is made on [date] 20

BETWEEN:

- (1) [insert name] of [insert address] (the “Sub-licensee”); and
- (2) [insert name] of [insert address] (the “Supplier” and together with the Supplier, the “Parties”).

WHEREAS:

- (A) [insert name of Authority] (the “Authority”) and the Supplier are party to a contract dated [insert date] (the “Contract”) for the provision by the Supplier of [insert brief description of services] to the Authority.
- (B) The Authority wishes to grant a sub-licence to the Sub-licensee in respect of certain software and intellectual property rights licensed to the Authority pursuant to the Contract (the “Sub-licence”).
- (C) It is a requirement of the Contract that, before the Authority grants such sub-licence to the Sub-licensee, the Sub-licensee execute a confidentiality agreement in favour of the Supplier in or substantially in the form of this Agreement to protect the Confidential Information of the Supplier.

IT IS AGREED as follows:

1 Interpretation

1.1 In this Agreement, unless the context otherwise requires:

“Confidential Information”

means:

- (a) Information, including all personal data within the meaning of the Data Protection Act 2018, and however it is conveyed, provided by the Authority to the Sub-licensee pursuant to or in connection with the Sub-licence that relates to:
 - (i) the Supplier; or
 - (ii) the operations, business, affairs, developments, intellectual property rights, trade secrets, know-how and/or personnel of the Supplier;
- (b) the source code and the object code of the software sub-licensed to the Sub-licensee pursuant to the Sub-licence together with

SCHEDULE 12 (SOFTWARE)

Confidential
 Contract for the provision of WAN Services

Security Classification (Official)
 Contract reference: [REDACTED]

build information, relevant design and development information, technical specifications of all functionality including those not included in standard manuals (such as those that modify system performance and access levels), configuration details, test scripts, user manuals, operating manuals, process definitions and procedures, and all such other documentation supplied by the Supplier to the Authority pursuant to or in connection with the Sub-licence;

- (c) other Information provided by the Authority pursuant to this Agreement to the Sub- licensee that is clearly designated as being confidential or equivalent or that ought reasonably to be considered to be confidential which comes (or has come) to the Sub- licensee’s attention or into the Sub- licensee’s possession in connection with the Sub-licence; and
- (d) Information derived from any of the above, but not including any Information that:
 - (a) was in the possession of the Sub- licensee without obligation of confidentiality prior to its disclosure by the Authority;
 - (b) was already generally available and in the public domain at the time of disclosure otherwise than by a breach of this Agreement or breach of a duty of confidentiality; or
 - (c) was independently developed without access to the Information;

“Information” means all information of whatever nature, however conveyed and in whatever form, including in writing, orally, by demonstration, electronically and in a tangible, visual or machine-readable medium (including CD-ROM, magnetic and digital form); and

“Sub-licence” has the meaning given to that expression in recital (B) to this Agreement.

SCHEDULE 12 (SOFTWARE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

1.2 In this Agreement:

- (a) a reference to any gender includes a reference to other genders;
- (b) the singular includes the plural and vice versa;
- (c) the words "include" and cognate expressions shall be construed as if they were immediately followed by the words "without limitation";
- (d) references to any statutory provision include a reference to that provision as modified, replaced, amended and/or re-enacted from time to time (before or after the date of this Agreement) and any prior or subsequent subordinate legislation made under it;
- (e) headings are included for ease of reference only and shall not affect the interpretation or construction of this Agreement; and
- (f) references to Clauses are to clauses of this Agreement.

2 Confidentiality Obligations**2.1 In consideration of the Authority entering into the Sub-licence, the Sub- licensee shall:**

- (a) treat all Confidential Information as secret and confidential;
- (b) have in place and maintain proper security measures and procedures to protect the confidentiality of the Confidential Information (having regard to its form and nature);
- (c) not disclose or permit the disclosure of any of the Confidential Information to any other person without obtaining the prior written consent of the Supplier or except as expressly set out in this Agreement;
- (d) not transfer any of the Confidential Information outside the United Kingdom;
- (e) not use or exploit any of the Confidential Information for any purpose whatsoever other than as permitted under the Sub-licence;
- (f) immediately notify the Supplier in writing if it suspects or becomes aware of any unauthorised access, copying, use or disclosure in any form of any of the Confidential Information; and
- (g) upon the expiry or termination of the Sub-licence:
 - (i) destroy or return to the Supplier all documents and other tangible materials that contain any of the Confidential Information;
 - (ii) ensure, so far as reasonably practicable, that all Confidential Information held in electronic, digital or other machine-readable form ceases to be readily accessible (other than by

SCHEDULE 12 (SOFTWARE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

the information technology staff of the Sub-licensee) from any computer, word processor, voicemail system or any other device; and

(iii) make no further use of any Confidential Information.

3 Permitted Disclosures

3.1 The Sub-licensee may disclose Confidential Information to those of its directors, officers, employees, consultants and professional advisers who:

- (a) reasonably need to receive the Confidential Information in connection with the Sub-licence; and
- (b) have been informed by the Sub-licensee of the confidential nature of the Confidential Information; and
- (c) have agreed to terms similar to those in this Agreement.

3.2 The Sub-licensee shall be entitled to disclose Confidential Information to the extent that it is required to do so by applicable law or by order of a court or other public body that has jurisdiction over the Sub-licensee.

3.3 Before making a disclosure pursuant to Clause 3.2, the Sub-licensee shall, if the circumstances permit:

- (a) notify the Supplier in writing of the proposed disclosure as soon as possible (and if possible before the court or other public body orders the disclosure of the Confidential Information); and
- (b) ask the court or other public body to treat the Confidential Information as confidential.

4 General

4.1 The Sub-licensee acknowledges and agrees that all property, including intellectual property rights, in Confidential Information disclosed to it by the Supplier shall remain with and be vested in the Supplier.

4.2 This Agreement does not include, expressly or by implication, any representations, warranties or other obligations:

- (a) to grant the Sub-licensee any licence or rights other than as may be expressly stated in the Sub-licence;
- (b) to require the Supplier to disclose, continue disclosing or update any Confidential Information; or
- (c) as to the accuracy, efficacy, completeness, capabilities, safety or any other qualities whatsoever of any Information or materials provided pursuant to or in anticipation of the Sub-licence.

4.3 The rights, powers and remedies provided in this Agreement are cumulative and not exclusive of any rights, powers or remedies provided by law. No

SCHEDULE 12 (SOFTWARE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

failure or delay by either Party to exercise any right, power or remedy will operate as a waiver of it nor will any partial exercise preclude any further exercise of the same, or of some other right, power or remedy.

- 4.4 Without prejudice to any other rights or remedies that the Supplier may have, the Sub-licensee acknowledges and agrees that damages alone may not be an adequate remedy for any breach by the Sub-licensee of any of the provisions of this Agreement. Accordingly, the Sub-licensee acknowledges that the Supplier shall be entitled to the remedies of injunction and specific performance as well as any other equitable relief for any threatened or actual breach of this Agreement and/or breach of confidence and that no proof of special damages shall be necessary for the enforcement of such remedies.
- 4.5 The maximum liability of the Sub-licensee to the Supplier for any breach of this Agreement shall be limited to ten million pounds (£10,000,000).
- 4.6 For the purposes of the Contracts (Rights of Third Parties) Act 1999 no one other than the Parties has the right to enforce the terms of this Agreement.
- 4.7 Each Party shall be responsible for all costs incurred by it or on its behalf in connection with this Agreement.
- 4.8 This Agreement may be executed in any number of counterparts and by the Parties on separate counterparts, but shall not be effective until each Party has executed at least one counterpart. Each counterpart shall constitute an original of this Agreement, but all the counterparts shall together constitute but one and the same instrument.

5 Notices

- 5.1 Any notice to be given under this Agreement (each a “**Notice**”) shall be given in writing and shall be delivered by hand and shall be deemed to have been duly given at the time of delivery provided that such Notice is sent to the relevant physical address, and expressly marked for the attention of the relevant individual, set out in Clause 5.2.

- 5.2 Any Notice:

- (a) if to be given to the Supplier shall be sent to:

[Address]

Attention: [Contact name and/or position, e.g. “The Finance Director”]

- (b) if to be given to the Sub-licensee shall be sent to:

[Name of Organisation]

[Address]

Attention: [REDACTED]

6 Governing law

SCHEDULE 12 (SOFTWARE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 6.1 This Agreement shall be governed by, and construed in accordance with, English law and any matter claim or dispute arising out of or in connection with this Agreement whether contractual or non-contractual, shall be governed by and determined in accordance with English law.
- 6.2 Each Party hereby irrevocably submits to the exclusive jurisdiction of the English courts in respect of any claim or dispute arising out of or in connection with this Agreement.

IN WITNESS of the above this Agreement has been signed by the duly authorised representatives of the Parties on the date which appears at the head of page 1.

For and on behalf of [name of Supplier]

Signature:	Date:

Name:	Position:

For and on behalf of [name of Sub-licensee]

Signature:	Date:

Name:	Position:

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 13

IMPLEMENTATION PLAN

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 13 (*Implementation Plan*)**PART A****1 INTRODUCTION****1.1** Part A of this Schedule:

- (a) defines the process for the preparation and implementation of the Outline Implementation Plan and Detailed Implementation Plan; and
- (b) identifies the Milestones (and associated Deliverables) including the Milestones which trigger payment to the Supplier of the applicable Milestone Payments following the issue of the applicable Milestone Achievement Certificate.

2 OUTLINE IMPLEMENTATION PLAN**2.1** The Outline Implementation Plan is set out in Annex 1.**2.2** All changes to the Outline Implementation Plan shall be subject to the Change Control Procedure provided that the Supplier shall not attempt to postpone any of the Milestones using the Change Control Procedure or otherwise (except in accordance with Clause 29 (*Authority Cause*)).**3 APPROVAL OF THE DETAILED IMPLEMENTATION PLAN****3.1** The Supplier shall submit a draft of the Detailed Implementation Plan to the Authority for approval within 20 Working Days of the Effective Date.**3.2** The Supplier shall ensure that the draft Detailed Implementation Plan:

- (a) incorporates all of the Milestones and Milestone Dates set out in the Outline Implementation Plan.
- (b) includes (as a minimum) the Supplier's proposed timescales in respect of the following:
 - (i) the completion of each design document;
 - (ii) the completion of the build phase;
 - (iii) the completion of any Testing to be undertaken in accordance with Schedule 14 (*Testing Procedures*); and
 - (iv) training and roll-out activities; and
 - (v) service acceptance activities;
- (c) clearly outlines all the steps required to implement the Milestones to be achieved in a maximum period of no more than 36 months,

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

together with a high-level plan for the rest of the programme, in conformity with the Authority Requirements;

- (d) clearly outlines the required roles and responsibilities of both Parties, including staffing requirements; and
- (e) is produced using a software tool as specified or agreed by the Authority (e.g. MS Project).

3.3 Prior to the submission of the draft Detailed Implementation Plan to the Authority in accordance with Paragraph 3.1, the Authority shall have the right:

- (a) to review any documentation produced by the Supplier in relation to the development of the Detailed Implementation Plan, including:
 - (i) any updates to the Supplier's Outline Implementation Plan;
 - (ii) details of the Supplier's intended approach to the Detailed Implementation Plan and its development;
 - (iii) copies of any drafts of the Detailed Implementation Plan produced by the Supplier; and
 - (iv) any other work in progress in relation to the Detailed Implementation Plan; and
- (b) to require the Supplier to include any reasonable changes or provisions in the Detailed Implementation Plan.

3.4 Following receipt of the draft Detailed Implementation Plan from the Supplier, the Authority shall:

- (a) review and comment on the draft Detailed Implementation Plan as soon as reasonably practicable; and
- (b) notify the Supplier in writing that it approves or rejects the draft Detailed Implementation Plan no later than 20 Working Days after the date on which the draft Detailed Implementation Plan is first delivered to the Authority.

3.5 If the Authority rejects the draft Detailed Implementation Plan:

- (a) the Authority shall inform the Supplier in writing of its reasons for its rejection; and
- (b) the Supplier shall then revise the draft Detailed Implementation Plan (taking reasonable account of the Authority's comments) and shall re-submit a revised draft Detailed Implementation Plan to the Authority for the Authority's approval within 10 Working Days of the date of the Authority's notice of rejection. The provisions of Paragraph 3.4 and this Paragraph 3.5 shall apply again to any resubmitted draft Detailed Implementation Plan, provided that either

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

- 3.6 If the Authority approves the draft Detailed Implementation Plan, it shall replace the Outline Implementation Plan from the date of the Authority's notice of approval. Any Authority Responsibilities set out in the Outline Implementation Plan will no longer apply and will be replaced by those set out in the Detailed Implementation Plan.

4 UPDATES TO AND MAINTENANCE OF THE DETAILED IMPLEMENTATION PLAN

- 4.1 Following the approval of the Detailed Implementation Plan by the Authority:
- (a) the Supplier shall submit a revised Detailed Implementation Plan to the Authority every 3 months starting 3 months from the Effective Date;
 - (b) without prejudice to Paragraph 4.1(a), the Authority shall be entitled to request a revised Detailed Implementation Plan at any time by giving written notice to the Supplier and the Supplier shall submit a draft revised Detailed Implementation Plan to the Authority within 20 Working Days of receiving such a request from the Authority (or such longer period as the Parties may agree provided that any failure to agree such longer period shall be referred to the Dispute Resolution Procedure);
 - (c) any revised Detailed Implementation Plan shall (subject to Paragraph 4.2) be submitted by the Supplier for approval in accordance with the procedure set out in Paragraph 3; and
 - (d) the Supplier's performance against the Implementation Plan shall be monitored at meetings of the Transition / Exit Board (as defined in Schedule 21 (*Governance*)). In preparation for such meetings, the current Detailed Implementation Plan shall be provided by the Supplier to the Authority not less than 5 Working Days in advance of each meeting of the Transition / Exit Board.
- 4.2 Save for any amendments which are of a type identified and notified by the Authority (at the Authority's discretion) to the Supplier in writing as not requiring approval, any material amendments to the Detailed Implementation Plan shall be subject to the Change Control Procedure provided that:
- (a) any amendments to elements of the Detailed Implementation Plan which are based on the contents of the Outline Implementation Plan shall be deemed to be material amendments; and
 - (b) in no circumstances shall the Supplier be entitled to alter or request an alteration to any Milestone Date except in accordance with Clause 29 (*Authority Cause*).

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

4.2B In relation to Milestones 13, 14, 15 and 16, the Supplier may request changes to the Detailed Implementation Plan to reschedule the cutover dates of Authority Sites where a Delay would otherwise be likely, by giving no less than 15 Working Days' notice in advance of the relevant Authority Sites' scheduled cutover dates. Such requests shall be considered by the Transition / Exit Board and approval by the Authority shall not be unreasonably withheld or delayed provided always that:

- a) such requests are limited to no more than 10% of the Authority Sites in scope of the relevant Milestone as at the first Approved version of the Detailed Implementation Plan; and
- b) if the requests involves moving Authority Site(s) from one Milestone to another Milestone, the number of Authority Sites moved to a later Milestone must be offset by the same number of Authority Sites being moved from a later Milestone into an earlier Milestone so that the total number of Authority Sites within each Milestone remains the same.

4.2C Changes requested under Paragraph 4.2B may include requests to move Authority Sites from one Milestone to another, subject to the number of Sites moved to a later Milestone being offset by the same number of Sites being moved from a later Milestone into an earlier one.

4.3 Any proposed amendments to the Detailed Implementation Plan shall not come into force until they have been approved in writing by the Authority.

5 GOVERNMENT REVIEWS

5.1 The Supplier acknowledges that the Services may be subject to Government review at key stages of the project. The Supplier shall cooperate with any bodies undertaking such review and shall allow for such reasonable assistance as may be required for this purpose within the Charges.

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

PART B**1 DOCUMENT APPROVAL PROCEDURE**

- 1.1 Except as expressly provided otherwise in this Contract, this Document Approval Procedure shall apply to the review and Approval of any Documentary Deliverable that the Supplier is required to provide under this Contract.
- 1.2 The Supplier shall ensure that all Documentary Deliverables are identified in the Implementation Plan and the relevant Project Work Order, or other relevant work-scoping document, including the timing of their delivery and review.
- 1.3 Where a third party, such as any Other Supplier, would reasonably be considered to have an interest in or a valid contribution to make towards a Documentary Deliverable, the Supplier shall ensure that such third party is consulted regarding its drafting.
- 1.4 This Document Approval Procedure commences with the agreement by the Parties of the Artefact Description for the relevant Documentary Deliverable.

Existing Artefact Descriptions for Documentary Deliverables

- 1.4A The Parties acknowledge and agree that the Artefact Descriptions listed in Annex 3 to this Schedule 13 are:
 - (a) already in existence and apply to the Documentary Deliverables required to be provided under this Contract; and
 - (b) shall be made available to the Supplier by the Authority on the Virtual Library.
- 1.4B Where a Artefact Description listed in Annex 3 applies to a Documentary Deliverable to be provided in connection with a Project, the relevant Project Work Order will identify the applicable Artefact Descriptions.

Development of Artefact Descriptions for Documentary Deliverables

- 1.5 Other than where the Artefact Description is already in existence under this Contract, where a Documentary Deliverable is subject to the Document Approval Procedure pursuant to Paragraph 1.1 of this Part B, the Supplier shall develop a draft Artefact Description materially in the format specified at Annex 2 to this Schedule 13 and/or in accordance with any applicable, more specific template Artefact Description under this Contract and shall make the draft Artefact Description available to the Authority for review.
- 1.6 The Supplier shall ensure that the Artefact Description is in a form approved by the Authority by any date specified in this Contract for this to have been achieved, or, in the absence of any such date being specified, in sufficient time to enable the applicable Documentary Deliverable to be delivered for review and to be Approved by the applicable date(s) for those activities.

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 1.7 The Authority shall review the draft Artefact Description in order to determine whether:
 - 1.7.1 it is in the format specified at Annex 2 to this Schedule 13; and
 - 1.7.2 the Authority believes that the Quality Criteria contained within the Artefact Description reflect the objective of the Documentary Deliverable and any requirements of this Contract that relate to the Documentary Deliverable.
- 1.8 The Authority shall undertake this review of the draft Artefact Description and shall notify the Supplier of the outcome of the review, within ten (10) Working Days of the Authority receiving the draft Artefact Description, or within such other period as may be agreed between the Parties.
- 1.9 Where the draft Artefact Description meets the criteria set out in Paragraph 1.7 of this Part B, the Authority shall notify its agreement of the Artefact Description in writing to the Supplier.
- 1.10 Where the draft Artefact Description does not meet such criteria, the Authority shall notify the Supplier, specifying the reasons why the draft has not been agreed.
- 1.11 If Paragraph 1.10 of this Part B applies, the Supplier shall liaise with the Authority to understand and complete the necessary changes and, subject to Paragraph 1.6 of this Part B, shall issue to the Authority within five (5) Working Days a revised draft Artefact Description, with all changes clearly highlighted.
- 1.12 For each Documentary Deliverable review, both Parties shall appoint a member of their organisation that shall act as the lead role in the active management of the progression of each draft Documentary Deliverable through to Approval.
- 1.13 The Authority may involve third parties in the review. In this event, the Authority may share draft Documentary Deliverables with such third parties and may invite them to participate in review meetings.
- 1.14 Other than to the extent already reflected in this Contract or agreed by the Parties, the Supplier shall propose for Approval by the Authority a Document Review Plan (which may be included in the Artefact Description), which will be consistent with the overall agreed timescale for development and Approval of the Documentary Deliverable.
- 1.15 The Document Review Plan will record the following dates:
 - 1.15.1 the First Draft Delivery Date;
 - 1.15.2 the date by which the Authority will notify the Supplier of the outcome of its review of the first draft and provide any review comments;
 - 1.15.3 the date by which the Authority and the Supplier will meet to review the comments;

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 1.15.4 the date by which the Supplier shall submit a revised draft Documentary Deliverable;
 - 1.15.5 the date by which the Authority shall check the revised draft; and
 - 1.15.6 the Planned Approval Date.
- 1.16 If the Supplier does not propose a Document Review Plan (or propose one acceptable to the Authority) by the applicable date in this Contract for this to occur (or, in the absence of such a date, in sufficient time to enable the applicable Documentary Deliverable to be delivered for review and to be Approved by the applicable date(s) for those activities), the Authority may specify the Document Review Plan.
- 1.17 The Parties shall conduct the review in accordance with the Document Review Plan and the timescales specified therein.
- 1.18 The Supplier shall produce and issue by the First Draft Delivery Date a complete draft Documentary Deliverable for review by the Authority, in accordance with the Document Review Plan.
- 1.19 The Supplier shall not submit a draft Documentary Deliverable for review by the Authority without first verifying that the draft Documentary Deliverable:
- 1.19.1 is in accordance with the format, scope and Quality Criteria specified in the applicable Artefact Description;
 - 1.19.2 is clearly written, in language that those parties who will need to refer to the document can understand;
 - 1.19.3 is complete, with an appropriate level of detail and any relevant cross-references; and
 - 1.19.4 has no obvious errors of spelling, grammar, numbering or order, duplications, or omissions.
- 1.20 The Authority shall review the draft Documentary Deliverable in order to determine whether it meets the applicable Quality Criteria or not and shall notify the Supplier of the outcome of this review, in accordance with the Document Review Plan.
- 1.21 Where the Authority review determines that the draft meets all the applicable Quality Criteria, the review shall be concluded at this point, and the Authority shall notify the Supplier of Approval Success in accordance with Paragraph 1.26 of this Part B.
- 1.22 Where the Authority rejects the draft Documentary Deliverable, because it does not meet all the applicable Quality Criteria or the Authority's requirements, the Authority shall specify its reasons for rejection in the form of collated review comments to the Supplier, and the following procedures shall apply:

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 1.22.1 the Parties shall meet to discuss the Authority's review comments and to agree and document the necessary changes to the draft Documentary Deliverable that are required to achieve Approval;
 - 1.22.2 the Supplier shall produce a revised draft Documentary Deliverable, incorporating all agreed changes, with changes clearly highlighted, for review by the Authority in accordance with the Document Review Plan; and
 - 1.22.3 the Authority shall review the revised draft Documentary Deliverable in order to determine whether the agreed changes have been made and whether the revised draft now meets the applicable Quality Criteria or not and shall notify the Supplier of the outcome of this review, in accordance with the Document Review Plan.
- 1.23 Where the Authority rejects the revised draft Documentary Deliverable, the Authority shall notify the Supplier of the reasons for its rejection of the draft. In this event, the Supplier shall liaise with the Authority to understand and complete the necessary changes and shall issue a further revised draft Documentary Deliverable for review and Approval.
- 1.24 The Supplier shall inform the Authority of any failure or likely failure to meet a date in the Document Review Plan as soon as such failure becomes known to the Supplier.
- 1.25 The Document Review Plan may only be changed with the Authority's prior written consent.

Approval Success

- 1.26 If all applicable Quality Criteria are met in accordance with the Document Approval Procedure and the applicable Document Review Plan, the Authority shall notify the Supplier of Approval Success as follows:
- 1.26.1 the Document Approval Procedure shall be recorded as successful where at the end of the review all the relevant Quality Criteria for the review are met and the Authority has notified the Supplier in writing by means of an Approval Certificate ("**Approval Success**").

Approval Failure

- 1.27 If all applicable Quality Criteria are not met by the Planned Approval Date and in accordance with the Document Approval Procedure, the Authority shall notify the Supplier of approval failure and the following shall apply:
- 1.27.1 the Document Approval Procedure shall record an approval failure where at the end of the review any of the relevant Quality Criteria for a review are not met ("**Approval Failure**"). The Authority may notify the Supplier of the reasons for such Approval Failure;
 - 1.27.2 where there is an Approval Failure pursuant to Paragraph 1.27.1 of this Part B, the Authority may fix revised dates in the Document

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Review Plan and the Supplier shall correct the errors which caused the Approval Failure, and the Document Approval Procedure shall be re-performed according to such revised dates;

- 1.27.3 if an Approval Failure (or any proposed extension to the Planned Approval Date following such Approval Failure) results in or is likely to result in the failure by the Supplier to Achieve a Milestone, then without prejudice to the Authority's other rights and remedies under this Contract, Clause 1.6 (Implementation Plan and Delays) shall apply as appropriate; and
- 1.27.4 each Party shall bear its own costs in respect of the Document Approval Procedure, unless there is an Approval Failure in which case the Supplier shall pay any costs incurred by the Authority in further review or re-trialling of a Documentary Deliverable pursuant to Paragraph 1.27.2 of this Part B or as a result of an Approval Failure.

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 1: OUTLINE IMPLEMENTATION PLAN

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
M1a – Mobilisation complete Documentary Deliverable	• Detailed Implementation Plan: approved in accordance with Paragraph 3 of Part A to this Schedule. • Transition governance approach: Approval Success. Quality Criteria to include: “aligned with Schedule 21 (<i>Governance</i>)”. • Knowledge transfer plan: Approval Success. • Project status report template: Approval Success. Quality Criteria to include: “meets needs of requirement 7.2.2.1 of the Transition Requirements”.	Effective Date + 35 Working Days	Convene the Transition / Exit Board to review ‘gate approval’ as described in the “Transition Framework” Standard	Not applicable

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
	• Transition Lead appointed. • Communications plan: Approval Success. Quality Criteria to include: “as specified in the Transition Requirements”. • The Supplier has provided confirmation that the Supplier Personnel on-boarding (in accordance with the requirement 7.1.1.3 Transition Requirements) is complete. • Quality Plans: provided in accordance with Clause 6.1. • Invoice template: Approval Success. Quality Criteria to include: “meets all invoice requirements of Schedule 15 (Charges and Invoicing)”.			

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (<i>if applicable</i>)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
	• Charging and invoicing processes: Approval Success. Quality Criteria to include: “meets all requirements of Schedule 15 (<i>Charges and Invoicing</i>)”. • Requirements traceability matrix (RTM): Approval Success. Quality Criteria to include: “in the format provided by the Authority”. • Information Management System boundary: diagram and supporting information provided by Supplier in accordance with Paragraph 4.2 of Schedule 5 (<i>Security Management</i>). • Security Management Plan: Approval Success. Quality Criteria to include: “structured in accordance with, and containing all the elements required by,			

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
	Paragraph 6.6 of Schedule 5 (<i>Security Management</i>)". • WAN Services Provisioning Process: Approval Success. Quality Criteria to include: "as described within the Transition Requirements". • Device logistics procedure: Approval Success. Quality Criteria to include: "as described in the Transition Requirements". • Transition Framework deliverables: the Parties have agreed the "Transition Framework" Documentary Deliverables relevant to the Implementation Services which correspond to the artefacts listed for each gate of the Transition Framework.			

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
	• “Gate Approval” of Gate 1 (‘Initiation and mobilisation’) as described in the “Transition Framework” Standard. • Artefact Descriptions for Documentary Deliverables required for Milestones M1a, M1b M2, M3, M4 and M5: Approval Success.			
M1b – Transitional Services mobilisation complete Documentary Deliverable Transitional Services	• Service continuity approach: Approval Success. Quality Criteria to include: "meets the needs of requirement 7.2.3 of the Transition Requirements." • The Supplier has provided the Authority with evidence which has been Approved by the Authority that it can operate the Transitional Services in accordance with	Effective Date + 40 Working Days		Not applicable

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
Commencement Date	Schedule 34 (Transitional Services). The Supplier has provided evidence of readiness for provision of the Transitional Services in accordance with the TS Performance Levels set out in Schedule 34 (Transitional Services).			
M2 – WAN Early Orders Documentary Deliverable	Early circuit order recommendation – Supplier has confirmed whether or not it recommends any early circuit orders, and the Authority has acknowledged the recommendation. Authority Site Access Request Process: Approval Success. Quality Criteria: “as described in the Transition Requirements.”	Effective Date + 35 Working Days		Not applicable

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (<i>if applicable</i>)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
M3 – Contract setup complete Documentary Deliverable	• In-flight project and interim service requests report: Approval Success. Quality Criteria to include: "meets the needs of requirement 7.1.1.13 of the Transition Requirements." Where the Authority requires the Supplier to take over the delivery of in-flight projects and service requests from the Preceding Services: The Supplier has produced Project Work Orders covering the required Project Work. • Other WAN Suppliers and completed Discovery Services list: Approval Success: Quality Criteria to include: "meets the needs of requirement 6.8.2 of the Service Management Requirements."	Effective Date + 40 Working Days	• Ensure that the information released to the Supplier is in a format that is capable of Supplier review. Provide details of Authority Assets for the Supplier to review and include in the Service Asset and Configuration Management System. • Release an in-flight project and interim service request list for Supplier assessment and review.	Not applicable

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (<i>if applicable</i>)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
	• Operational Interlock Document: Approval Success. Quality Criteria to include: “as described in the Service Management Requirements”. • Service Assets and Configuration Items baseline list: Approval Success. Quality Criteria to include: “as described in the Service Management Requirements.” and “Service Assets and Configuration Items list will include the Operational Services and Transitional Services, Service Assets and Configuration Items including Transferring Assets where applicable. The list will baseline the Service Assets and Configuration Items” and “list of Approved Service Assets uploaded			

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
	by Supplier to the Authority's CMDB. • Product and Services Catalogue: Approval Success. Quality Criteria to include: "meets all the requirements of Schedule 15 (Charges and Invoicing)."			
M4 – High Level Design Documentary Deliverable	• High Level Design: Approval Success. • WAN Cutover Approach: Approval Success. Quality Criteria: "as described in the Transition Requirements". • Artefact Descriptions for the Milestone M6: Approval Success.	Effective Date + 46 Working Days		Not applicable
M5 - Service and Solution	• Service Design Package: Approval Success. Quality Criteria to include: "aligned with the	Effective Date + 56 Working Days	• Providing input into the Service Design Packages and detailing how the	Not applicable

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
Design complete Documentary Deliverable	Service Management Requirements.” • The Supplier has with Authority input completed the review of the Performance Indicator for Capacity Management. • Training plan: Approval Success. Quality Criteria to include the training of Authority nominated service operations personnel covering how the Operational Services operate and how they will integrate with the Authority’s operations. • Solution Design: Approval Success. Quality Criteria to include: “aligned with the Technical Requirements.” • The Supplier has agreed with the Authority the early life support		Authority’s service management environment operates. • Attendance as reasonably required to support the Supplier’s ITSM Toolset integration workshops. • Input into the scoping of the IT Health Check	

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
	period for each Service and the Authority Site migrations. • Security Management Plan (new iteration): Residual Risk Statement issued following a Security Assurance Decision in accordance with Schedule 5 (<i>Security Management</i>). Note: The Supplier shall not be required to procure an IT Health Check prior to submission of this version of the Security Management Plan. • Social Value Delivery Plan: Approval Success. Quality Criteria to include: “meets all requirements of the Social Value Requirements.”			
M6 – Low Level Designs complete	• WAN connectivity Low Level Design: Approval Success.	Effective Date + 58 Working Days	• Convene the Transition / Exit Board to review ‘gate approval’ as described in	Not applicable

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
Documentary Deliverable	Quality Criteria to include: “aligned with the Technical Requirements.” • Gateway Services Low Level Design: Approval Success. Quality Criteria: The Supplier has completed due diligence of the low level design covering the Transitional Services which are equivalent to the Gateway Services and has confirmed the Low Level Design for the Gateway Services. • Core Network Services Low Level Design: Approval Success. Quality Criteria to include: “aligned with the Technical Requirements.” • “Gate Approval” of Gate 2 (‘Detailed Design Complete’) as described in the “Transition Framework” Standard.		the “Transition Framework” Standard.	

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
	• Artefact Descriptions for Documentary Deliverables required for Milestone M7, M8 and M9: Approval Success. • Achievement of Milestones M1a, M1b, M2, M3, M4 and M5.			
M7 – ITSM Toolset setup and integration Documentary Deliverable	• The Supplier has successfully completed the setup of its ITSM Toolset. • The Supplier has successfully tested connectivity to the Authority's network, in line with the Approved High-Level Design and Solution Design. • Test data: Approval Success: Quality Criteria to include: meets all the requirements of Schedule 14 (Testing Procedures).	Effective Date + 109 Working Days		Not applicable

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
	The Supplier has successfully completed IT service management toolset integration, where applicable, with the ITSM Toolset and successfully tested integration in accordance with the Service Management Requirements.			
M8 – Operational Services testing sign off Documentary Deliverable	Test Specification: Approval Success. Quality Criteria to include: “meets all the requirements of paragraph 7 of Schedule 14 (Testing Procedures)”. Test Report: Approval Success. Quality Criteria to include: “meets the requirements of Schedule 14 (Testing Procedures)”. Test Certificates: Approved by the Authority in accordance with Schedule 14 (Testing Procedures)	Effective Date + 109 Working Days		Not applicable

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
	for all Tests required to be carried out in respect of the establishment of the Operational Services as documented in the Test Strategy and Test Plans, including: ○ The Supplier IT service management toolset integration complete where applicable (e-bonding and operational monitoring integration with the ITSM Toolset). ○ The Supplier support resources have been granted all necessary security clearance. ○ The Supplier has provided Operational Services policies and procedures covering WAN Connectivity, Gateway Services, Core Network Services and Field Services, and these have			

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
	been tested to evidence that they are capable of integration with the Authority service management processes and procedures. • Service management processes and procedures: Approval Success. ○ The Supplier has provided evidence that the Other WAN Supplier service management is being undertaken in accordance with requirement 6.8.2 of the Service Management Requirements) including the establishment and testing of Operational Interlock Documents. • Knowledge transfer plan: Approval Success.			

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
	○ The Supplier resource on boarding is complete. ○ The Supplier has confirmed that training of the Supplier service management teams is complete (in accordance with Schedule 14 (<i>Testing Procedures</i>)). ● WAN service management acceptance Testing has been completed covering service management and operational processes testing (including testing Supplier IT service management toolset integration with the ITSM Toolset and the synchronisation of performance data across the toolsets (in accordance with Schedule 14 (Testing Procedures)) ● Artefact Descriptions for Documentary Deliverables			

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
	required for Milestone M10: Approval Success. Achievement of Milestones M2, M3, M4, M5, M6 and M7.			
M9 Operational Services security sign off – Documentary Deliverable	Security Management Plan: Residual Risk Statement issued following a Security Assurance Decision in accordance with Schedule 5 (<i>Security Management</i>).	Effective Date + 112 Working Days		Not applicable
M10 Operational Services acceptance Non – Documentary Deliverable ATP Milestone	- ITSCM awareness and training: delivered in accordance with Paragraph 6.3.4.5 of the Service Management Requirements. Training material and knowledge articles: Approval Success. Service Validation and Testing Report: Approval Success. Quality	Effective Date + 122 Working Days	- Schedule and chair Service Readiness Reviews. - Convene the Transition / Exit Board to review ‘gate approval’ as described in the “Transition Framework” Standard.	ATP Milestone - Yes Key Milestone - Yes

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
The Supplier must have Achieved this Milestone 10 before it can commence provision of the relevant Operational Services Operational Services Commencement Date Key Milestone (Y)	Criteria to include: "Evidence that the Supplier can provide the Operational Services to meet the Target Performance Levels" and in accordance with Schedule 14 (Testing Procedures)". • Requirements Traceability Matrix (RTM) updated: Approval Success. • Risk Register updated: Approval Success. • Project Work Orders: Where the Authority has agreed updates to the Risk Register, and where additional Services are required to mitigate risk impacts, the Supplier has produced Project Proposals covering the required Services. • The Supplier has provided evidence of readiness to Achieve			

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (<i>if applicable</i>)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
	Operational Service Commencement Date for the WAN Connectivity and Core Network Services and Field Services, and its readiness to provide such Services to meet or exceed the Target Performance Levels for each relevant Performance Indicator. • “Gate Approval” of Gate 3 (‘Build and Test’) and Gate 4 (‘Cutover to Service Commencement’) as described in the “Transition Framework” Standard. • Artefact Descriptions for Documentary Deliverables required for Milestones M11 and M12: Approval Success. • Achievement of Milestones M8 and M9.			

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
M11 – Gateway Services Transition Documentary Deliverable ATP Milestone The Supplier must have Achieved Milestone 10 before it can commence provision of the relevant Operational Services Operational Services	Transition of Gateway Services from the Transitional Services to the Operational Services has been completed, including (in respect of the Gateway Services only): • Gateway Services cutover plan: Approval Success. • Management and support for the Gateway System retained from the Transitional Services for Gateway Services. • Post Go Live Report: Approval Success. Quality Criteria to include: “as specified within the requirements in Paragraph 7.2.1.7 of the Transition Requirements. and provides evidence that the Supplier can operate the Services	Effective Date + 138 Working Days	• Facilitate Supplier access to infrastructure in accordance with Paragraph 2.1(e) of Schedule 7 (<i>Authority Responsibilities</i>), to support the managed take on of the in-scope gateways infrastructure. • Convene the Transition / Exit Board to review ‘gate approval’ as described in the “Transition Framework” Standard.	Key Milestone - Yes

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
Commencement Date Key Milestone (Y)	in accordance with Schedule 3 (Performance Levels)". • The Supplier has provided evidence of readiness to Achieve Operational Service Commencement Date for the Gateway Services, and provision of the Services to meet or exceed the Target Performance Levels for each relevant Performance Indicator. • "Gate Approval" of Gate 5 ('Handover to BAU') as described in the "Transition Framework" Standard. • Achievement of Milestone M10.			
M12 – Pilot site transitions	• The pilot Authority Sites have been transitioned and the Supplier has evidenced that all the site types	Effective Date + 159 Working Days	• Nominate pilot migration Authority Sites.	ATP Milestone – Yes

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
Non - Documentary Deliverable As part of Transition Milestone M12, the Supplier will be expected to deliver into Service a combination of pilot site types from the Authority Site List covering a range of the Authority's business functions and site types. The combination of	and business functions included within the pilot can be successfully transitioned. • The Supplier has evidenced and validated the redundancy, failover and full diversity of Transport Services at each Authority Site where delivered, in accordance with requirement 3.2.1.5 of the Technical Requirements. • Pilot Authority Sites have been transitioned into Business as Usual (BAU) support. • Lessons learned report: Approval Success. Quality Criteria to include: "The Supplier has provided a pilot site transitions lesson learned report covering key findings and making recommendations for changes to	(The pilot site transitions will have a duration of up to 45 Working Days)	• Convene the Transition / Exit Board to review 'gate approval' as described in the "Transition Framework" Standard. • The Authority shall arrange for the delivery to the Supplier of the relevant SD-WAN Edge Devices (as set out in AO-009 in Schedule 7) in accordance with the Detailed Implementation Plan.	Key Milestone - Yes

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
pilot sites for delivery as part of this Milestone will be agreed as within the WAN site lifecycle approach and migration plan. The expectation is that the number of pilot sites should not exceed more than three percent of the total Authority site list. Commencement of the pilot site transitions are	the deployment approach, with an accompanying Impact Assessment and planning and scheduling updates”. • Post Go Live Report: Approval Success: Quality Criteria to include: “as specified in requirements in Paragraph 7.1.2.7 of the Transition Requirements”. • The Supplier has provided evidence that for the Transitioned Sites Operational Services have been implemented, and its readiness to provide the Operational Services to meet or exceed the Target Performance Levels for each relevant Performance Indicator. • The Supplier has provided the required information to support the			

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
not dependent on Achievement of Milestone M11 – Gateway Services Transition Operational Services Commencement Date for Operational Services per Authority Site ATP Milestone The Supplier must have Achieved this Milestone 12 before it can	issue of a Milestone Achievement Certificate by the Authority. • “Gate Approval” of Gate 5 (‘Handover to BAU’) as described in the “Transition Framework” Standard. • Artefact Descriptions for Documentary Deliverables required for Milestones M13, M14, M15 and M16: Approval Success. • Achievement of Milestone M10.			

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
commence provision of the relevant Operational Services				
M13 – Site transitions phase 1 Non - Documentary Deliverable Operational Services Commencement Date for Operational Services per Authority Site	• Site transitions phase 1 cutover plan: Approval Success. • The Authority Sites set out in the Site transitions phase 1 cutover plan have been transitioned. • Phase 1 Authority Sites have been transitioned into Business as Usual (BAU) support. • The Supplier has evidenced and validated the redundancy, failover and full diversity of Transport Services at each Authority Site where delivered, in accordance	Effective Date + 236 Working Days	• Convene the Transition / Exit Board to review 'gate approval' as described in the "Transition Framework" Standard. • The Authority shall arrange for the delivery to the Supplier of the relevant SD-WAN Edge Devices (as set out in AO-009 in Schedule 7) in accordance with the Detailed Implementation Plan.	Key Milestone - Yes

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
As part of Transition Milestone M13, the Supplier will be expected to deliver into Service a combination of site types from the Authority Site List. The combination of site types for delivery as part of this Milestone will be agreed as within the Site transitions phase 1 cutover plan.	with requirement 3.2.1.5 of the Technical Requirements. • Post Go Live Report: Approval Success. Quality Criteria to include: “as specified within the requirements in 7.1.2.7 of the Transition Requirements.” • The Supplier has provided evidence that for the Transitioned Sites Operational Services have been implemented, and its readiness to provide the Operational Services to meet or exceed the Target Performance Levels for each relevant Performance Indicator. Site Transition Certificates issued for all Authority Sites in phase 1. • “Gate Approval” of Gate 5 (‘Handover to BAU’) as described			

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
The Supplier must have Achieved Milestones M10 and M12 before it can commence provision of the relevant Operational Services Key Milestone (Y)	in the “Transition Framework” Standard. • The Supplier has provided the required information to support the issue of a Milestone Achievement Certificate by the Authority. • Site-specific low-level configuration designs: Approval Success. Quality Criteria to include: “aligned with the Technical Requirements” and “designs cover all Transitioned Sites”. • Achievement of Milestones M10 and M12.			
M14 – Site transitions phase 2	• Site transitions phase 2 cutover plan: Approval Success.	Effective Date + 318 Working Days	• Convene the Transition / Exit Board to review ‘gate approval’ as described in the “Transition Framework” Standard.	Key Milestone - Yes

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
Non - Documentary Deliverable Operational Services Commencement Date for Operational Services per Authority Site As part of Transition Milestone M14, the Supplier will be expected to deliver into Service a combination of site types from	• The Authority Sites set out in the Site transitions phase 2 cutover plan have been transitioned. • The phase 2 Authority Sites have been transitioned into Business as Usual (BAU) support. • The Supplier has evidenced and validated the redundancy, failover and full diversity of Transport Services at each Authority Site where delivered, in accordance with requirement 3.2.1.5 of the Technical Requirements. • Post Go Live Report: Approval Success. Quality Criteria to include: "as specified in requirement 7.1.2.7 of the Transition Requirements". • The Supplier has provided evidence that for the Transitioned		• The Authority shall arrange for the delivery to the Supplier of the relevant SD-WAN Edge Devices (as set out in AO-009 in Schedule 7) in accordance with the Detailed Implementation Plan.	

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
the Authority Site List. The combination of site types for delivery as part of this Milestone will be agreed as within the Site transitions phase 2 cutover plan. The Supplier must have Achieved this Milestone 14 before it can commence provision of the relevant Operational Services	Sites Operational Services have been implemented, and its readiness to provide the Operational Services to meet or exceed the Target Performance Levels for each relevant Performance Indicator. Site Transition Certificates issued for all Authority Sites in phase 2. • The Supplier has provided the required information to support the issue of a Milestone Achievement Certificate by the Authority. • Site-specific low-level configuration designs: Approval Success. Quality Criteria to include: “aligned with the Technical Requirements” and “designs cover all Transitioned Sites”.			

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
Key Milestone (Y)	• “Gate Approval” of Gate 5 (‘Handover to BAU’) as described in the “Transition Framework” Standard. • Achievement of Milestones M10 and M12.			
M15 – Site transitions phase 3 Non - Documentary Deliverable Operational Services Commencement Date for Operational Services Per Authority Site	• Site transitions phase 3 cutover plan: Approval Success. • The Authority Sites set out in the Site transitions phase 3 cutover plan have been transitioned. • The Supplier has evidenced and validated the redundancy, failover and full diversity of Transport Services at each Authority Site where delivered, in accordance with requirement 3.2.1.5 of the Technical Requirements.	Effective Date + 400 Working Days	• Convene the Transition / Exit Board to review ‘gate approval’ as described in the “Transition Framework” Standard. • The Authority shall arrange for the delivery to the Supplier of the relevant SD-WAN Edge Devices (as set out in AO-009 in Schedule 7) in accordance with the Detailed Implementation Plan.	Key Milestone - Yes

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
As part of Transition Milestone M15, the Supplier will be expected to deliver into Service a combination of site types from the Authority Site List. The combination of site types for delivery as part of this Milestone will be agreed as within the Site transitions phase 3 cutover plan.	- Phase 3 Authority Sites have been transitioned into Business as Usual (BAU) support. Post Go Live Report: Approval Success. Quality Criteria to include: "as specified in requirements 7.1.2.7 of the Transition Requirements". - The Supplier has provided evidence that for the Transitioned Sites Operational Services have been implemented, and its readiness to provide the Operational Services to meet or exceed the Target Performance Levels for each relevant Performance. Site Transition Certificates issued for all Authority Sites in phase 3.			

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
The Supplier must have Achieved this Milestone M15 before it can commence provision of the relevant Operational Services Key Milestone (Y)	- The Supplier has provided the required information to support the issue of a Milestone Achievement Certificate by the Authority. Site-specific low-level configuration designs: Approval Success. Quality Criteria to include: “aligned with the Technical Requirements” and “designs cover all Transitioned Sites”. “Gate Approval” of Gate 5 (‘Handover to BAU’) as described in the “Transition Framework” Standard. - Achievement of Milestones M10 and M12.			
M16 Site transitions phase 4	Site transitions phase 4 cutover plan: Approval Success.	Effective Date + 482 Working Days	Convene the Transition / Exit Board to review ‘gate approval’ as described in	CPP Milestone – Yes

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
Non - Documentary Deliverable Operational Services Commencement Date for Operational Services per Authority Site As part of Transition Milestone M16, the Supplier will be expected to deliver into Service a combination of site types from the Authority Site List. The	• The Authority Sites set out in the Site transitions phase 4 Sites cutover plan have been transitioned. • The Supplier has evidenced and validated the redundancy, failover and full diversity of Transport Services at each Authority Site where delivered, in accordance with requirement 3.2.1.5 of the Technical Requirements. • Phase 4 Authority Sites have been transitioned into Business as Usual (BAU) support. • Post Go Live Report: Approval Success. Quality Criteria to include: "as specified in requirement 7.1.2.7 of the Transition Requirements".		the "Transition Framework" Standard. • The Authority shall arrange for the delivery to the Supplier of the relevant SD-WAN Edge Devices (as set out in AO-009 in Schedule 7) in accordance with the Detailed Implementation Plan.	Key Milestone - Yes

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
combination of site types for delivery as part of this Milestone will be agreed as within the Site transitions phase 4 cutover plan. The Supplier must have Achieved this Milestone 16 before it can commence provision of the relevant Operational Services	• The Supplier has provided evidence that for the Transitioned Sites Operational Services have been implemented, and its readiness to provide the Operational Services to meet or exceed the Target Performance Levels for each relevant Performance Indicator. Site Transition Certificates issued for all Authority Sites in phase 4. • The Supplier has provided the required information to support the issue of a Milestone Achievement Certificate by the Authority. • Site-specific low-level configuration designs: Approval Success. Quality Criteria to include: “aligned with the Technical			

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
CPP Milestone (Y) Key Milestone (Y)	Requirements” and “designs cover all Transitioned Sites”. • “Gate Approval” of Gate 5 (‘Handover to BAU’) as described in the “Transition Framework” Standard. • Artefact Descriptions for the Milestone M17: Approval Success. • Achievement of Milestones M13, M14 and M15.			
M17 – Transition Complete Non - Documentary Deliverable	• Achievement of Milestones M12, M13, M14, M15 and M16. • Lessons learned report: Approval Success. • Transition closure report: Approval Success.	Effective Date + 507 Working Days	• Convene the Transition / Exit Board to review ‘gate approval’ as described in the “Transition Framework” Standard.	Key Milestone - Yes

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone	Deliverables (<i>bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone</i>)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/ CPP Key Milestone, subject to Delay Payments (Y/N)
Key Milestone (Y)	“Gate Approval” of Gate 6 (‘Transition Complete’) as described in the “Transition Framework” Standard.			

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 2
FORMAT FOR ARTEFACT DESCRIPTIONS

FOR

DOCUMENTARY DELIVERABLES

<u>ARTEFACT REFERENCE</u>	
Title of Deliverable	
Purpose of Deliverable	
Project or Programme	
Scope of Deliverable	
Format & Presentation of Deliverable	
Composition of Deliverable	
Derivation of Deliverable	
Allocated to	
Quality Criteria for Deliverable	
Quality Method	
People or skills required	
First Draft Delivery Date for Deliverable	
Planned Successful Approval Date for Deliverable	

SCHEDULE 13 (IMPLEMENTATION PLAN)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 3
EXISTING ARTEFACT DESCRIPTIONS

FOR

DOCUMENTARY DELIVERABLES

<u>ARTEFACT DESCRIPTION TITLE</u>	<u>DOCUMENT DETAILS INCLUDING FILE NAME AND VERSION NUMBER</u>
Project Status Report	AD Project Status Report v1.0 dated 08 Sept 2025
Communications Plan	AD Communications Plan v1.0 dated 08 Sept 2025
Service Assets and Configuration Items baseline list	AD Baseline Asset and CI Listv1.0 dated 08 Sept 2025
Knowledge Transfer Plan	AD Knowledge Transfer Plan v1.0 dated 08 Sept 2025
Operational Interlock Document	AD Operational Interlock Document v1.0 dated 08 Sept 2025
WAN Cutover Approach	AD WAN Cutover Approach v1.0 dated 08 Sept 2025
Quality Plan	AD Quality Plan v1.0 dated 08 Sept 2025
WAN Services Provisioning Process	AD WAN Services Provisioning Process v1.0 dated 08 Sept 2025
Service Design Package (SDP)	AD Service Design Package v1.0 dated 08 Sept 2025
Security Management Plan	AD Security Management Planv1.0 dated 08 Sept 2025
Solution Design	AD Solution Design v1.0 dated 08 Sept 2025
Requirements Traceability Matrix	AD Requirements Traceability Matrix v1.0 dated 08 Sept 2025
High-Level Design (HLD)	AD High-Level Design v1.0 dated 08 Sept 2025

SCHEDULE 14 (TESTING PROCEDURES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 14

TESTING PROCEDURES

SCHEDULE 14 (TESTING PROCEDURES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Schedule 14 (*Testing Procedures*)

1 DEFINITIONS

In this Schedule, the following definitions shall apply:

“Component”	any constituent parts of the infrastructure for a Service, hardware or Software;
“Material Test Issue”	a Test Issue of Severity Level 1 or Severity Level 2;
“Severity Level”	the level of severity of a Test Issue, the criteria for which are described in Annex 1;
“Test Certificate”	a certificate materially in the form of the document contained in Annex 2 issued by the Authority when a Non-Documentary Deliverable has satisfied its relevant Test Success Criteria;
“Test Issue”	any variance or non-conformity of a Non-Documentary Deliverable from its requirements (such requirements being set out in the relevant Test Success Criteria);
“Test Issue Threshold”	in relation to the Tests applicable to a Milestone, a maximum number of Severity Level 3, Severity Level 4 and Severity Level 5 Test Issues as set out in the relevant Test Plan;
“Test Issue Management Log”	a log for the recording of Test Issues as described further in Paragraph 9.1;
“Test Plan”	a plan: (a) for the Testing of Non-Documentary Deliverables; and (b) setting out other agreed criteria related to the achievement of Milestones, as described further in Paragraph 5;
“Test Reports”	the reports to be produced by the Supplier setting out the results of Tests;
“Test Specification”	the specification that sets out how Tests will demonstrate that the Test Success Criteria have

SCHEDULE 14 (TESTING PROCEDURES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

been satisfied, as described in more detail in Paragraph 7;

“Test Strategy”	a strategy for the conduct of Testing as described further in Paragraph 4;
“Test Success Criteria”	in relation to a Test, the test success criteria for that Test as referred to in Paragraph 6;
“Test Witness”	any person appointed by the Authority pursuant to Paragraph 10.1; and
“Testing Procedures”	the applicable testing procedures and Test Success Criteria set out in this Schedule.

2 RISK

2.1 The issue of a Test Certificate, a Milestone Achievement Certificate, a conditional Milestone Achievement Certificate and/or a Site Transition Certificate shall not:

- (a) operate to transfer any risk that the relevant Deliverable, Milestone or Service is complete or will meet and/or satisfy the Authority's requirements for that Deliverable, Milestone or Service; or
- (b) affect the Authority's right subsequently to reject:
 - (i) all or any element of the Deliverables to which a Test Certificate relates;
 - (ii) any Milestone to which the Milestone Achievement Certificate relates; or
 - (iii) all or any element of the Services to which a Site Transition Certificate relates.

2.2 Notwithstanding the issuing of any Milestone Achievement Certificate (including the Milestone Achievement Certificate in respect of Authority to Proceed), the Supplier shall remain solely responsible for ensuring that:

- (a) the Supplier Solution as designed and developed is suitable for the delivery of the Services and meets the Authority Requirements;
- (b) the Services are implemented in accordance with this Contract; and
- (c) each Target Performance Level is met from the relevant Operational Service Commencement Date.

3 TESTING OVERVIEW

3.1 All Tests conducted by the Supplier shall be conducted in accordance with the Test Strategy, the Test Plans and the Test Specifications.

SCHEDULE 14 (TESTING PROCEDURES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 3.2 The Supplier shall not submit any Non-Documentary Deliverable for Testing:
- (a) unless the Supplier is reasonably confident that it will satisfy the relevant Test Success Criteria;
 - (b) until the Authority has issued a Test Certificate in respect of any prior, dependant Non-Documentary Deliverable(s); and
 - (c) until the Parties have agreed the Test Plan and the Test Specification relating to the relevant Non-Documentary Deliverable(s).
- 3.3 The Supplier shall use reasonable endeavours to submit each Non-Documentary Deliverable for Testing or re-Testing by or before the date set out in the Implementation Plan for the commencement of Testing in respect of the relevant Non-Documentary Deliverable.
- 3.4 Prior to the issue of a Test Certificate, the Authority shall be entitled to review the relevant Test Reports and the Test Issue Management Log.
- 3.5 Any Disputes between the Authority and the Supplier regarding Testing shall be referred to the Dispute Resolution Procedure using the Expedited Dispute Timetable.

4 TEST STRATEGY

- 4.1 The Supplier shall develop the final Test Strategy as soon as practicable after the Effective Date but in any case no later than 20 Working Days (or such other period as the Parties may agree in writing) after the Effective Date.
- 4.2 The final Test Strategy shall include:
- (a) an overview of how Testing will be conducted in accordance with the Implementation Plan;
 - (b) the process to be used to capture and record Test results and the categorisation of Test Issues;
 - (c) the method for mapping the expected Test results to the Test Success Criteria;
 - (d) the procedure to be followed if a Non-Documentary Deliverable fails to satisfy the Test Success Criteria or produces unexpected results, including a procedure for the resolution of Test Issues;
 - (e) the procedure to be followed to sign off each Test;
 - (f) the process for the production and maintenance of Test Reports and reporting, including templates for the Test Reports and the Test Issue Management Log, and a sample plan for the resolution of Test Issues;

SCHEDULE 14 (TESTING PROCEDURES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (g) the names and contact details of the Authority's and the Supplier's Test representatives;
- (h) a high level identification of the resources required for Testing, including facilities, infrastructure, personnel and Authority and/or third party involvement in the conduct of the Tests;
- (i) the technical environments required to support the Tests; and
- (j) the procedure for managing the configuration of the Test environments.

5 TEST PLANS

5.1 The Supplier shall develop Test Plans and submit these for the approval of the Authority as soon as practicable but in any case no later than 20 Working Days (or such other period as the Parties may agree in the Test Strategy or otherwise agree in writing) prior to the start date for the relevant Testing (as specified in the Implementation Plan).

5.2 Each Test Plan shall include as a minimum:

- (a) the relevant Test definition and the purpose of the Test, the Milestone to which it relates, the requirements being tested and, for each Test, the specific Test Success Criteria to be satisfied;
- (b) a detailed procedure for the Tests to be carried out, including:
 - (i) the timetable for the Tests, including start and end dates;
 - (ii) the Testing mechanism;
 - (iii) dates and methods by which the Authority can inspect Test results or witness the Tests in order to establish that the Test Success Criteria have been met;
 - (iv) the mechanism for ensuring the quality, completeness and relevance of the Tests;
 - (v) the format and an example of Test progress reports and the process with which the Authority accesses daily Test schedules;
 - (vi) the process which the Authority will use to review Test Issues and the Supplier's progress in resolving these in a timely basis;
 - (vii) the Test schedule;
 - (viii) the re-Test procedure, the timetable and the resources which would be required for re-Testing; and
- (c) the process for escalating Test Issues from a re-test situation to the taking of specific remedial action to resolve the Test Issue.

SCHEDULE 14 (TESTING PROCEDURES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 5.3 The Authority shall not unreasonably withhold or delay its approval of the Test Plans provided that the Supplier shall incorporate any reasonable requirements of the Authority in the Test Plans.

6 TEST SUCCESS CRITERIA

The Test Success Criteria for:

- (a) each Test that must be Achieved for the Supplier to Achieve either the ATP Milestone or a CPP Milestone are set out in Annex 4; and
- (b) all other Tests shall be agreed between the Parties as part of the relevant Test Plan pursuant to Paragraph 5.

7 TEST SPECIFICATION

- 7.1 Following approval of a Test Plan, the Supplier shall develop the Test Specification for the relevant Non-Documentary Deliverables as soon as reasonably practicable and in any event at least 10 Working Days (or such other period as the Parties may agree in the Test Strategy or otherwise agree in writing) prior to the start of the relevant Testing (as specified in the Implementation Plan).

- 7.2 Each Test Specification shall include as a minimum:

- (a) the specification of the Test data, including its source, scope, volume and management, a request (if applicable) for relevant Test data to be provided by the Authority and the extent to which it is equivalent to live operational data;
- (b) a plan to make the resources available for Testing;
- (c) Test scripts;
- (d) Test pre-requisites and the mechanism for measuring them; and
- (e) expected Test results, including:
 - (i) a mechanism to be used to capture and record Test results; and
 - (ii) a method to process the Test results to establish their content.

8 TESTING

- 8.1 Before submitting any Non-Documentary Deliverables for Testing the Supplier shall subject the relevant Non-Documentary Deliverables to its own internal quality control measures.
- 8.2 The Supplier shall manage the progress of Testing in accordance with the relevant Test Plan and shall carry out the Tests in accordance with the relevant Test Specification. Tests may be witnessed by the Test Witnesses in accordance with Paragraph 10.

SCHEDULE 14 (TESTING PROCEDURES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 8.3 The Supplier shall notify the Authority at least 10 Working Days (or such other period as the Parties may agree in writing) in advance of the date, time and location of the relevant Tests and the Authority shall ensure that the Test Witnesses attend the Tests, except where the Authority has specified in writing that such attendance is not necessary.
- 8.4 The Authority may raise and close Test Issues during the Test witnessing process.
- 8.5 The Supplier shall provide to the Authority in relation to each Test:
- (a) a draft Test Report not less than 2 Working Days (or such other period as the Parties may agree in writing) prior to the date on which the Test is planned to end; and
 - (b) the final Test Report within 5 Working Days (or such other period as the Parties may agree in writing) of completion of Testing.
- 8.6 Each Test Report shall provide a full report on the Testing conducted in respect of the relevant Non-Documentary Deliverables, including:
- (a) an overview of the Testing conducted;
 - (b) identification of the relevant Test Success Criteria that have been satisfied;
 - (c) identification of the relevant Test Success Criteria that have not been satisfied together with the Supplier's explanation of why those criteria have not been met;
 - (d) the Tests that were not completed together with the Supplier's explanation of why those Tests were not completed;
 - (e) the Test Success Criteria that were satisfied, not satisfied or which were not tested, and any other relevant categories, in each case grouped by Severity Level in accordance with Paragraph 9.1; and
 - (f) the specification for any hardware and software used throughout Testing and any changes that were applied to that hardware and/or software during Testing.

9 TEST ISSUES

- 9.1 Where a Test Report identifies a Test Issue, the Parties shall agree the classification of the Test Issue using the criteria specified in Annex 1 and the Test Issue Management Log maintained by the Supplier shall log Test Issues reflecting the Severity Level allocated to each Test Issue.
- 9.2 The Supplier shall be responsible for maintaining the Test Issue Management Log and for ensuring that its contents accurately represent the current status of each Test Issue at all relevant times. The Supplier shall make the Test Issue Management Log available to the Authority upon request.

SCHEDULE 14 (TESTING PROCEDURES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 9.3 The Authority shall confirm the classification of any Test Issue unresolved at the end of a Test in consultation with the Supplier. If the Parties are unable to agree the classification of any unresolved Test Issue, the Dispute shall be dealt with in accordance with the Dispute Resolution Procedure using the Expedited Dispute Timetable.

10 TEST WITNESSING

- 10.1 The Authority may, in its sole discretion, require the attendance at any Test of one or more Test Witnesses selected by the Authority, each of whom shall have appropriate skills to fulfil the role of a Test Witness.
- 10.2 The Supplier shall give the Test Witnesses access to any documentation and Testing environments reasonably necessary and requested by the Test Witnesses to perform their role as a Test Witness in respect of the relevant Tests.
- 10.3 The Test Witnesses:
- (a) shall actively review the Test documentation;
 - (b) will attend and engage in the performance of the Tests on behalf of the Authority so as to enable the Authority to gain an informed view of whether a Test Issue may be closed or whether the relevant element of the Test should be re-Tested;
 - (c) shall not be involved in the execution of any Test;
 - (d) shall be required to verify that the Supplier conducted the Tests in accordance with the Test Success Criteria and the relevant Test Plan and Test Specification;
 - (e) may produce and deliver their own, independent reports on Testing, which may be used by the Authority to assess whether the Tests have been Achieved;
 - (f) may raise Test Issues on the Test Issue Management Log in respect of any Testing; and
 - (g) may require the Supplier to demonstrate the modifications made to any defective Non-Documentary Deliverable before a Test Issue is closed.

11 TEST QUALITY AUDIT

- 11.1 Without prejudice to its rights pursuant to Clause 12.2(b) (*Records, Reports, Audits & Open Book Data*), the Authority may perform on-going quality audits in respect of any part of the Testing (each a "**Testing Quality Audit**") subject to the provisions set out in the agreed Quality Plan.
- 11.2 The focus of the Testing Quality Audits shall be on:
- (a) adherence to an agreed methodology;

SCHEDULE 14 (TESTING PROCEDURES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (b) adherence to the agreed Testing process;
 - (c) adherence to the Quality Plan;
 - (d) review of status and key development issues; and
 - (e) identification of key risk areas.
- 11.3 The Supplier shall allow sufficient time in the Test Plan to ensure that adequate responses to a Testing Quality Audit can be provided.
- 11.4 The Authority will give the Supplier at least 5 Working Days' written notice of the Authority's intention to undertake a Testing Quality Audit and the Supplier may request, following receipt of that notice, that any Testing Quality Audit be delayed by a reasonable time period if in the Supplier's reasonable opinion, the carrying out of a Testing Quality Audit at the time specified by the Authority will materially and adversely impact the Implementation Plan.
- 11.5 A Testing Quality Audit may involve document reviews, interviews with the Supplier Personnel involved in or monitoring the activities being undertaken pursuant to this Schedule, the Authority witnessing Tests and demonstrations of the Non-Documentary Deliverables to the Authority. Any Testing Quality Audit shall be limited in duration to a maximum time to be agreed between the Supplier and the Authority on a case by case basis (such agreement not to be unreasonably withheld or delayed). The Supplier shall provide all reasonable necessary assistance and access to all relevant documentation required by the Authority to enable it to carry out the Testing Quality Audit.
- 11.6 If the Testing Quality Audit gives the Authority concern in respect of the Testing Procedures or any Test, the Authority shall:
- (a) discuss the outcome of the Testing Quality Audit with the Supplier, giving the Supplier the opportunity to provide feedback in relation to specific activities; and
 - (b) subsequently prepare a written report for the Supplier detailing its concerns,
- and the Supplier shall, within a reasonable timeframe, respond in writing to the Authority's report.
- 11.7 In the event of an inadequate response to the Authority's report from the Supplier, the Authority (acting reasonably) may withhold a Test Certificate (and consequently delay the grant of a Milestone Achievement Certificate) until the issues in the report have been addressed to the reasonable satisfaction of the Authority.
- 12 OUTCOME OF TESTING**
- 12.1 The Authority shall issue a Test Certificate as soon as reasonably practicable when the Non-Documentary Deliverables satisfy the Test Success Criteria in respect of that Test without any Test Issues.

SCHEDULE 14 (TESTING PROCEDURES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 12.2 If the Non-Documentary Deliverables (or any relevant part) do not satisfy the Test Success Criteria then the Authority shall notify the Supplier and:
- (a) the Authority may issue a Test Certificate conditional upon the remediation of the Test Issues;
 - (b) where the Parties agree that there is sufficient time prior to the relevant Milestone Date, the Authority may extend the Test Plan by such reasonable period or periods as the Parties may reasonably agree and require the Supplier to rectify the cause of the Test Issue and re-submit the Non-Documentary Deliverables (or the relevant part) to Testing; or
 - (c) where the failure to satisfy the Test Success Criteria results, or is likely to result, in the failure (in whole or in part) by the Supplier to meet a Milestone, then without prejudice to the Authority's other rights and remedies, such failure shall constitute a Notifiable Default for the purposes of Clause 25.1 (*Rectification Plan Process*).
- 12.3 The Authority shall be entitled, without prejudice to any other rights and remedies that it has under this Contract, to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing which is required for the Test Success Criteria for that Non-Documentary Deliverable to be satisfied.
- 13 ISSUE OF MILESTONE ACHIEVEMENT CERTIFICATE**
- 13.1 The Authority shall issue a Milestone Achievement Certificate in respect of a given Milestone as soon as is reasonably practicable following:
- (a) the issuing by the Authority of Test Certificates and/or conditional Test Certificates in respect of all Non-Documentary Deliverables related to that Milestone which are due to be Tested; and
 - (b) the issuing by the Authority of Approval Certificates pursuant to Paragraph 1.26 of Part B of Schedule 13 (Implementation Plan) in respect of Documentary Deliverables related to that Milestone that are not due to be Tested but which have met all their Quality Criteria;
 - (c) performance by the Supplier to the reasonable satisfaction of the Authority of any other tasks identified in the Implementation Plan as associated with that.
- 13.2 The grant of a Milestone Achievement Certificate shall entitle the Supplier to the receipt of a payment in respect of that Milestone in accordance with the provisions of Schedule 15 (*Charges and Invoicing*).
- 13.3 If a Milestone is not Achieved, the Authority shall promptly issue a report to the Supplier setting out:

SCHEDULE 14 (TESTING PROCEDURES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (a) the applicable Test Issues ; and
 - (b) any other reasons for the relevant Milestone not being Achieved.
- 13.4 If there are Test Issues but these do not exceed the Test Issues Threshold, then provided there are no Material Test Issues, the Authority shall issue a Milestone Achievement Certificate.
- 13.5 Without prejudice to the Authority's other remedies the following shall constitute a Notifiable Default for the purposes of Clause 25.1 (*Rectification Plan Process*) and the Authority shall refuse to issue a Milestone Achievement Certificate where:
 - (a) there is one or more Material Test Issue(s); or
 - (b) the information required under Schedule 24 (*Reports and Records Provisions*) (*Annex 3: Records to Upload To Virtual Library*) has not been uploaded to the Virtual Library in accordance with Paragraph 3 of that Schedule.
- 13.6 If there are Test Issues which exceed the Test Issues Threshold but there are no Material Test Issues, the Authority may at its discretion (without waiving any rights in relation to the other options) choose to issue a Milestone Achievement Certificate conditional on the remediation of the Test Issues in accordance with an agreed Rectification Plan provided that:
 - (a) any Rectification Plan shall be agreed before the issue of a conditional Milestone Achievement Certificate unless the Authority agrees otherwise (in which case the Supplier shall submit a Rectification Plan for approval by the Authority within 10 Working Days of receipt of the Authority's report pursuant to Paragraph 13.3); and
 - (b) where the Authority issues a conditional Milestone Achievement Certificate, it may (but shall not be obliged to) revise the failed Milestone Date and any subsequent Milestone Date.

14 ISSUE OF A SITE TRANSITION CERTIFICATE

- 14.1 Where the Supplier has completed all applicable Implementation Services for the transition of an Authority Site into Operational Service the Supplier shall:
 - (a) carry out applicable Tests in accordance with this Schedule 14 and any relevant Test Plan; and
 - (b) provide to the Authority evidence that the relevant Authority Site meets the requirements of this Contract for Operational Service to commence, including:
 - (i) evidence that all Implementation Services have been completed in accordance with the Implementation Plan, Schedule 13 (implementation) and Schedule 2 Annex C (Transition Requirements);

SCHEDULE 14 (TESTING PROCEDURES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (ii) evidence that the Test Success Criteria have been met and there are no Test Issues beyond those specified in the Transition Requirements as being permitted;
 - (iii) copies of Milestone Achievement Certificates for any applicable ATP Milestones; and
 - (iv) an Approved Post Go Live Report for the Authority Site in accordance with the Transition Requirements.
- 14.2 The Authority will review such evidence and, subject to Paragraph 14.3, issue a Site Transition Certificate in the form set out in Annex 5 to this Schedule 14.
- 14.3 The Supplier shall provide any additional information or assistance reasonably requested by the Authority in order to satisfy it that a Site Transition Certificate can be issued in respect of an Authority Site.

SCHEDULE 14 (TESTING PROCEDURES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 1: TEST ISSUES – SEVERITY LEVELS

- 1 Severity Level 1 Test Issue:** a Test Issue that causes non-recoverable conditions, e.g. it is not possible to continue using a Component, a Component crashes, there is database or file corruption, or data loss;
- 2 Severity Level 2 Test Issue:** a Test Issue for which, as reasonably determined by the Authority, there is no practicable workaround available, and which:
 - 2.1 causes a Component to become unusable;
 - 2.2 causes a lack of functionality, or unexpected functionality, that has an impact on the current Test; or
 - 2.3 has an adverse impact on any other Component(s) or any other area of the Services;
- 3 Severity Level 3 Test Issue:** a Test Issue which:
 - 3.1 causes a Component to become unusable;
 - 3.2 causes a lack of functionality, or unexpected functionality, but which does not impact on the current Test; or
 - 3.3 has an impact on any other Component(s) or any other area of the Services;

but for which, as reasonably determined by the Authority, there is a practicable workaround available;
- 4 Severity Level 4 Test Issue:** a Test Issue which causes incorrect functionality of a Component or process, but for which there is a simple, Component based, workaround, and which has no impact on the current Test, or other areas of the Services; and
- 5 Severity Level 5 Test Issue:** a Test Issue that causes a minor problem, for which no workaround is required, and which has no impact on the current Test, or other areas of the Services.

SCHEDULE 14 (TESTING PROCEDURES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 2: TEST CERTIFICATE

To: **[NAME OF SUPPLIER]**

FROM: **[NAME OF AUTHORITY]**

[Date]

Dear Sirs,

TEST CERTIFICATE

Non-Documentary Deliverables: **[insert description of Non-Documentary Deliverables]**

We refer to the agreement (the “**Contract**”) relating to the provision of the Services between the **[name of Authority]** (the “**Authority**”) and **[name of Supplier]** (the “**Supplier**”) dated **[date]**.

Capitalised terms used in this certificate have the meanings given to them in Schedule 1 (*Definitions*) or Schedule 14 (*Testing Procedures*) of the Contract.

[We confirm that the Non-Documentary Deliverables listed above have been tested successfully in accordance with the Test Plan relevant to those Non-Documentary Deliverables.]

OR

[This Test Certificate is issued pursuant to Paragraph 12.1 of Schedule 14 (*Testing Procedures*)

of the Contract on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]*

**delete as appropriate*

Yours faithfully

[Name]

[Position]

acting on behalf of **[name of Authority]**

SCHEDULE 14 (TESTING PROCEDURES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 3: MILESTONE ACHIEVEMENT CERTIFICATE

To: **[NAME OF SUPPLIER]**

FROM: **[NAME OF AUTHORITY]**

[Date]

Dear Sirs,

MILESTONE ACHIEVEMENT CERTIFICATE

Milestone: **[insert description of Milestone]**

We refer to the agreement (the “**Contract**”) relating to the provision of the Services between the **[name of Authority]** (the “**Authority**”) and **[name of Supplier]** (the “**Supplier**”) dated **[date]**.

Capitalised terms used in this certificate have the meanings given to them in Schedule 1 (Definitions) or Schedule 14 (*Testing Procedures*) of the Contract.

[We confirm that all the Deliverables relating to Milestone **[number] have been:**

- (i) **in the case of Non-Documentary Deliverables, tested successfully in accordance with the Test Plan relevant to this Milestone [or that a conditional Test Certificate has been issued in respect of those Deliverables that have not satisfied the relevant Test Success Criteria.]]***; and
- (ii) **in the case of Documentary Deliverables, reviewed and all the relevant Quality Criteria for the review have been met.**

OR

[This Milestone Achievement Certificate is granted pursuant to Paragraph 13.1 of Schedule 14 (*Testing Procedures*) of the Contract on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]*

[You may now issue an invoice in respect of the Milestone Payment associated with this Milestone in accordance with the provisions of Schedule 15 (Charges and Invoicing)]*

**delete as appropriate*

Yours faithfully

[Name]

[Position]

acting on behalf of **[Authority]**

SCHEDULE 14 (TESTING PROCEDURES)

Confidential
 Contract for the provision of WAN Services

Security Classification (Official)
 Contract reference: [REDACTED]

ANNEX 4: TEST SUCCESS CRITERIA

1 Tests to be Achieved in order to Achieve the ATP Milestone

ATP Milestone Name	Test	Pre-conditions*	Test Success Criteria
M10 WAN services acceptance	- Supplier operational support processes for the WAN services - Supplier operational processes integrate with the Authority's service management processes	The Supplier has achieved Milestone Achievement Certificate sign off for Milestones 1, 2, 3, 4, 5, 6, 7, 8 and 9	- Service Management Acceptance Testing sign off, of the WAN service management and operational processes. Including testing the Supplier ITSM Toolset integration with the Authority's ITSM Toolset, and the synchronisation of performance data across the ITSM Toolsets - The Supplier has completed the Authority approved ITSCM Awareness and Training for all ITSCM related personnel - Supplier provides the Authority with evidence which is capable of Approval that they can operate Services in line with the Schedule 3 (Performance Levels) - Achieved Operational Service Commencement for the WAN Services, and provision of the Services to meet or exceed the Target Performance Levels for each relevant

SCHEDULE 14 (TESTING PROCEDURES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ATP Milestone Name	Test	Pre-conditions*	Test Success Criteria
			Performance Indicator (Schedule 3 Performance Levels)
M12 – Pilot site transitions	• Test WAN connectivity from the gateway to the Authority WAN pilot Sites • Test high availability and full diversity of transport services at each Authority pilot Site where delivered	• The Supplier has achieved Milestone Achievement Certificate sign off for Milestone 10	• The Supplier successfully tested connectivity from the Gateway to the Authority WAN pilot sites. • The Supplier has evidenced and validated the high availability and full diversity of transport services at each Authority Site where delivered • Pilot Authority Sites transitioned into Business as Usual (BAU) support.

SCHEDULE 14 (TESTING PROCEDURES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

2 Tests to be Achieved in order to Achieve a CPP Milestone

CPP Milestone Charge No.	Test	Test Success Criteria
M17 – Transition complete	• Supplier lessons learned report review and approval • Supplier Transition closure report review and Approval	• The Supplier has achieved Milestone Achievement Certificate sign off for Milestones 12, 13,14, 15 and 16 • Supplier lessons learned report Approval • Supplier Transition closure report Approval • The Supplier has evidenced closure of its Transition project

SCHEDULE 14 (TESTING PROCEDURES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 5: SITE TRANSITION CERTIFICATE

To: **[NAME OF SUPPLIER]**

FROM: **[NAME OF AUTHORITY]**

[Date]

To Whom It May Concern,

SITE TRANSITION CERTIFICATE

Site Transition complete and in receipt of the Operational Services: **[Authority Site Name]**

We refer to the agreement (the “**Contract**”) relating to the provision of the Services between the **[name of Authority]** (the “**Authority**”) and **[name of Supplier]** (the “**Supplier**”) dated **[date]**.

Capitalised terms used in this certificate have the meanings given to them in Schedule 1 (*Definitions*) or Schedule 14 (*Testing Procedures*) of the Contract.

In accordance with Paragraph 14.2 of Schedule 14 (*Testing Procedures*), we confirm that **[Authority Site Name]** in accordance with the **[cutover plan name]** and **[Request for Change reference]** has been tested successfully in accordance with the Test Plan and has Achieved the requirements for Operational Service to commence.

The Operational Service Commencement Date for **[Authority Site Name]** is: **[insert date of this certificate]**.

Yours faithfully

[Name]

[Position]

acting on behalf of **[name of Authority]**

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 15

CHARGES AND INVOICING

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 15 (*Charges and Invoicing*)

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

“Achieved Profit Margin”	the cumulative Supplier Profit Margin calculated from (and including) the Effective Date (or, if applicable, the date of the last adjustment to the Charges made pursuant to Paragraph 2.2 of Part D (<i>Excessive Supplier Profit Margin</i>) of this Schedule 15) to (and including) the last day of the previous Contract Year;
“Access Circuit Charges”	has the meaning given in Paragraph 4.3.5(a);
“Annual Shortfall Payment”	has the meaning given in Paragraph 4.3.5(b);
“Annual Shortfall Percentage”	has the meaning given in Paragraph 4.5.3(c);
“Annual Volume Variance”	has the meaning given in Paragraph 4.5.3(d);
“Anticipated Contract Life Profit Margin”	the anticipated Supplier Profit Margin over the Term as reflected in the Financial Model;
“Average Weekly Earnings”	means the “Average weekly earnings – regular pay, Great Britain” as published by the Office for National Statistics;
“Catalogue Item Charges”	has the meaning given to it in Paragraph 4.4 of Part A (<i>Pricing</i>) of this Schedule 15;
“Certificate of Costs”	a certificate of costs signed by the Supplier’s Chief Financial Officer or Director of Finance (or equivalent as agreed in writing by the Authority in advance of issue of the relevant certificate) and substantially in the format set out in Annex D (<i>Pro-forma Certificate of Costs</i>);
“Circuit Baseline Date”	has the meaning given in Paragraph 4.3.5(e);
“Circuit Initial Term”	has the meaning given in Paragraph 4.3.4(a);
“Consumed”	means: (a) in respect of time and materials resource, the

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

deployment of that resource by the Supplier in the course of providing the relevant Services to the Authority; and

- (b) in respect of Catalogue Items, the fulfilment of the relevant Catalogue Item,

and "**Consumption**" shall be construed accordingly;

"Costs"

the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Services:

- (a) the cost to the Supplier or the Key Sub-contractor (as the context requires), calculated per Work Day, of engaging the Supplier Personnel, including:
 - (i) base salary paid to the Supplier Personnel;
 - (ii) employer's national insurance contributions;
 - (iii) Employer Pension Contributions;
 - (iv) car allowances;
 - (v) any other contractual employment benefits;
 - (vi) staff training;
 - (vii) workplace accommodation;
 - (viii) workplace IT equipment and tools reasonably necessary to perform the Services (but not including items included within limb (b) below); and
 - (ix) reasonable recruitment costs, as agreed with the Authority;
- (b) costs incurred in respect of those Assets which are detailed on the Registers and which would be treated as capital costs according to generally accepted accounting principles within the UK, which shall include the cost to be charged in respect of Assets by the Supplier to the Authority or (to the extent that risk and title in any Asset is not held by the Supplier) any cost actually incurred by the Supplier in respect of those Assets;
- (c) operational costs which are not included within (a) or (b) above, to the extent that such costs are

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

necessary and properly incurred by the Supplier in the delivery of the Services;

- (d) Forecast Contingency Costs;
- (e) Reimbursable Expenses to the extent these are incurred in delivering any Services where the Charges for those Services are to be calculated on a Fixed Price or Firm Price pricing mechanism;

but excluding:

- (i) Overhead;
- (ii) financing or similar costs;
- (iii) maintenance and support costs to the extent that these relate to maintenance and/or support services provided beyond the Term, whether in relation to Assets or otherwise;
- (iv) taxation;
- (v) fines and penalties;
- (vi) amounts payable under Schedule 17 (*Benchmarking*); and
- (vii) non-cash items (including depreciation, amortisation, impairments and movements in provisions);

“Delay Payment Cap”

[REDACTED];

“Delay Payment Rate”

has the meaning given in in Paragraph 1.1(a) of Part C (*Adjustments to the Charges and Risk Register*) of this Schedule 15;

“Deemed Forecast Annual Circuit Charges”

has the meaning given in Paragraph 4.3.5(f)

“Employer Pension Contributions”

means:

- (a) in respect of CSPS Eligible Employees those sums set out at Clauses 7.1.1 (*annual administration charges covering core services*), 7.1.5 (*employer contributions*), 7.1.7 (*the ASLC*) and 7.1.8 (*flat charges applicable to the Partnership Pension Account*) of the Admission Agreement;

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (b) in respect of NHSPS Eligible Employees, the standard employer contribution rate applicable to NHS Pension Scheme employers during the Term and payable by the Supplier (but no other costs, contributions, charges or surcharges payable by the Supplier to or in respect of the NHS Pension Scheme or in respect of any NHS Premature Retirement Rights, unless otherwise agreed in writing by the Authority);
- (c) in respect of LGPS Eligible Employees the standard employer contribution rate applicable to LGPS Eligible Employees during the Term and payable by the Supplier (but no other costs, contributions, charges or surcharges payable by the Supplier to or in respect of the LGPS or in respect of any Beckmann Liabilities, unless otherwise agreed in writing by the Authority); and

such other employer pension contributions, charges or costs incurred by the Supplier which have been expressly agreed by the Authority in writing to constitute 'Employer Pension Contributions';

“Excess Construction Charges” or “ECCs”

has the meaning given in Paragraph 8.1 of Part A (*Pricing*) of this Schedule 15;

“European Standard”

in relation to an electronic invoice means the European standard and any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870.

“Final TUPE Information”

has the meaning given in Paragraph 8.3 of Part C (*Adjustments to the Charges and Risk Register*) of this Schedule 15;

“Fixed Service Charges”

has the meaning given to it in Paragraph 4.2 of Part A (*Pricing*) of this Schedule 15;

“Forecast Annual Circuit Charges”

has the meaning given in Paragraph 4.3.5(g);

“Forecast Contingency Costs”

the costs which the Supplier forecasts may be incurred in relation to the risks and contingencies that are identified in the Risk Register, such costs being those set out in the column headed 'Forecast Contingency Costs' in the Risk Register (as such costs are updated from time to time);

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

“Forecast Period”	has the meaning given in Paragraph 4.3.5(h);
“Gateway Service Charges”	has the meaning given in Paragraph 4.2.2(a) of Part A (<i>Pricing</i>) of this Schedule 15;
“Gateway Test System Charges”	has the meaning given in Paragraph 4.2.2(b) of Part A (<i>Pricing</i>) of this Schedule 15;
“Guaranteed Maximum Price”	in relation to a Milestone, 110% of the Target Price for the relevant Milestone;
“Incurred Costs”	in relation to a Milestone, the sum of: (a) the fixed day costs set out in the relevant Project Work Order multiplied by the number of Work Days that have been expended by the Supplier Personnel in Achieving the relevant Milestone; and (b) any amount that would fall within limbs (b) or (c) of the definition of “Costs” (but subject to exceptions (i) to (vii) in that definition), to the extent that such amount has been incurred in Achieving the relevant Milestone;
“Indexation” and “Index”	the adjustment of an amount or sum in accordance with Paragraph 5 (<i>Indexation</i>) of Part C (<i>Adjustments to the Charges and Risk Register</i>) of this Schedule 15;
“Initial TUPE Information”	has the meaning given in Paragraph 8.1 of Part C (<i>Adjustments to the Charges and Risk Register</i>) of this Schedule 15;
“Key Milestone”	the Milestones identified in Annex A (<i>Key Milestones, Payment Milestones, Milestone Payments and Delay Payments</i>) to this Schedule 15 as key milestones and in respect of which Delay Payments may be payable in accordance with Paragraph 1 (<i>Delay Payments</i>) of Part C (<i>Adjustments to the Charges and Risk Register</i>) of this Schedule 15 if the Supplier fails to Achieve the Milestone Date in respect of such Milestone;
“Linked Milestone”	has the meaning given in Paragraph 3.3 of Part A (<i>Pricing</i>) of this Schedule 15;
“Maximum Permitted Profit Margin”	the Anticipated Contract Life Profit Margin plus 5%;

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

“Milestone Group” has the meaning given in Paragraph 3.6 of Part B (Project Charges) of this Schedule 15;

“Milestone Retention” for each Milestone shall be calculated as follows:

- (a) where the Milestone Payment for the relevant Milestone is determined by reference to a fixed pricing mechanism or on a Time and Materials basis, 20% of the Milestone Payment for that Milestone; and
- (b) where the Milestone Payment for the relevant Milestone is determined by reference to a Guaranteed Maximum Price with Target Cost pricing mechanism, 20% of the Target Price for the Milestone,

and, in the case of a Key Milestone, prior to deduction from the Milestone Payment of any Delay Payment attributable to that Key Milestone and without taking account of any amount payable by the Supplier pursuant to Paragraph 1.2 of Part C (*Adjustments to the Charges and Risk Register*) of this Schedule 15;

“Milestone Retention Fund” has the meaning given in Paragraph 3.6 of Part A (*Pricing*) of this Schedule 15;

“Monthly Service Charges” has the meaning given in Paragraph 5.3 of Part A (*Pricing*) of this Schedule 15;

“Overhead” those amounts which are intended to recover a proportion of the Supplier’s or the Key Sub-contractor’s (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Personnel and accordingly included within limb (a) of the definition of “Costs” or the day cost set out in the relevant Project Work Order;

“Part Year” has the meaning given in Paragraph 4.3.5.1;

“Payment Milestone” a Milestone identified as a Payment Milestone in the table in Annex A (*Key Milestones, Payment Milestones, Milestone Payments and Delay Payments*) to this Schedule 15;

“Payment Planner” means a report provided by the Supplier in respect of each Service Period to the Authority containing

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

information on historical and forecast consumption and the associated Charges;

“Reconciliation Report”

has the meaning given in Paragraph 8.6 of Part C (*Adjustments to the Charges and Risk Register*) of this Schedule 15;

“Reimbursable Expenses”

reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance with the Authority’s expenses policy current from time to time, but not including:

- (a) travel expenses incurred as a result of Supplier Personnel travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Authority otherwise agrees in advance in writing; and
- (b) subsistence expenses incurred by Supplier Personnel whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed;

“Service Charges”

means the charges calculated in accordance with Paragraph 4 (*Service Charges*) of Part A (*Pricing*) of this Schedule 15;

“Service Credit Point Value”

means the value for each Service Point as calculated in accordance with Paragraph 3.7 of Part C (*Adjustments to the Charges and Risk Register*) of this Schedule 15;

“Supplier Profit”

in relation to a period or a Milestone (as the context requires), the difference between the total Charges (in nominal cash flow terms but excluding any Deductions) and total Costs (in nominal cash flow terms) for the relevant period or in relation to the relevant Milestone;

“Supplier Profit Margin”

in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage;

“Supporting Documentation”

sufficient information in writing to enable the Authority reasonably to assess whether the Charges, Reimbursable Expenses and other sums due from the Authority detailed

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

in the information are properly payable, including copies of any applicable Milestone Achievement Certificates or receipts;

“Target Cost”	the target Cost for the relevant Milestone as set out in the relevant Project Work Order or Change Authorisation Note;
“Target Price”	the target Charge for the relevant Milestone as set out in the relevant Project Work Order or Change Authorisation Note;
“Transport Service Charges”	has the meaning given in Paragraph 4.3.2(a) of Part A (<i>Pricing</i>) of this Schedule 15;
“Verification Period”	in relation to an Allowable Assumption, the period from (and including) the Effective Date to (and including) the date at which the relevant Allowable Assumption expires, as set out against the relevant Allowable Assumption in column 11 in Table 14 of Annex F (<i>Allowable Assumptions</i>);
“Volume Based Service Charges”	has the meaning given to it in Paragraph 4.3 of Part A (<i>Pricing</i>) of this Schedule 15;
“Work Day”	8 Work Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day;
“Work Hours”	the hours spent by the Supplier Personnel properly working on the Services including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks.

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Part A: Pricing**1 APPLICABLE PRICING MECHANISM**

1.1 Except as is agreed by the Parties pursuant to the Change Control Procedure, the only Charges payable by the Authority in respect of the performance by the Supplier of its obligations under this Contract are:

1.1.1 the Milestone Payments payable in accordance with Paragraph 3 of this Part A;

1.1.2 the Service Charges payable in accordance with Paragraph 4 of this Part A; and

1.1.3 Project Charges payable in accordance with Part B (*Project Charges*) of this Schedule 15.

2 TRANSITIONAL SERVICES

2.1 The Authority shall pay the Supplier for performance of the Transitional Services in accordance with Schedule 34 (*Transitional Services*).

3 MILESTONE PAYMENTS

3.1 The Milestone Payments are charged on a fixed price basis and are set out in the table in Annex A (*Key Milestones, Payment Milestones, Milestone Payments and Delay Payments*) to this Schedule 15.

3.2 Subject to Paragraph 3.3 below and the provisions of Part C (*Adjustments to the Charges and Risk Register*) of this Schedule 15 in relation to the deduction of Delay Payments, following the Achievement of a Payment Milestone the Supplier shall be entitled to invoice the Authority for the Milestone Payment associated with that Payment Milestone less the applicable Milestone Retention.

3.3 Where it is identified in the table in Annex A (*Key Milestones, Payment Milestones, Milestone Payments and Delay Payments*) to this Schedule 15 that a Payment Milestone is linked to Achievement of a previous Milestone(s) ("**Linked Milestone**"), the Supplier shall only be entitled to invoice the Authority for the Milestone Payment associated with that Payment Milestone if the Authority has issued a Milestone Achievement Certificate in respect of the Linked Milestone(s).

3.4 Each invoice relating to a Milestone Payment shall be supported by a Milestone Achievement Certificate and all relevant Supporting Information.

3.5 The Milestone Payments shall not be subject to Indexation.

Release of Milestone Retentions

3.6 Each Milestone Retention deducted from a Milestone Payment shall be combined with previous Milestone Retention(s) deducted from Milestone

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Payment(s) relating to Payment Milestone(s) which have already been Achieved by the Supplier to form the “**Milestone Retention Fund**”.

- 3.7 On Achievement of each of Milestone 13, Milestone 14 and Milestone 15 and Milestone 16, the Supplier shall be entitled to invoice the Authority for an amount equal to 20% of the value of the Milestone Retention Fund as at the date immediately prior to Achievement of the relevant Milestone less any Delay Payments deducted in accordance with Paragraph 1.2 of Part C (*Adjustments to the Charges and Risk Register*) of this Schedule 15. So, by way of example, on Achievement of Milestone 13, then (assuming all previous Milestones have been Achieved) the Supplier shall be entitled to 20% of the Milestone Retention Fund which at that point will comprise 20% of the Milestone Payment for Milestone 6 + 20% of the Milestone Payment for Milestone 10 + 20% of the Milestone Payment for Milestone 11.
- 3.8 On Achievement of (Milestone 16 (Site Transition – Phase 4)), the Supplier shall be entitled to invoice the Authority for an amount equal to the remaining value of the Milestone Retention Fund less any Delay Payments deducted in accordance with Paragraph 1.2 of Part C (*Adjustments to the Charges and Risk Register*) of this Schedule 15.

4 SERVICE CHARGES

- 4.1 The Service Charges shall be payable by the Authority to the Supplier and shall comprise:
- 4.1.1 the **Fixed Service Charges** (calculated in accordance with Paragraph 4.2 below); and
 - 4.1.2 the **Volume Based Service Charges** (calculated in accordance with Paragraph 4.3 below); and
 - 4.1.3 the **Catalogue Item Charges** (calculated in accordance with Paragraph 4.4 below).
- 4.2 **Fixed Service Charges**
- 4.2.1 The Fixed Service Charges payable by the Authority are set out in Paragraph 1 (*Fixed Service Charges*) of Annex B (*Service Charges*) to this Schedule 15.
 - 4.2.2 Fixed Service Charges shall comprise:
 - (a) the Service Charges for the provision of the Gateway Services as set out in Paragraph 1.1 of Annex B (*Service Charges*) to this Schedule 15 (“**Gateway Service Charges**”);
 - (b) the Service Charges for the provision of the Gateway Test System as set out in Paragraph 1.1 of Annex B (*Service Charges*) to this Schedule 15 (“**Gateway Test System Charges**”); and

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (c) the Service Charges for the provision of the relevant Optional Services as set out in Paragraph 1.3 of Annex B (Service Charges) to this Schedule 15.

4.2.3 The Gateway Service Charges and the Gateway Test System Charges shall be subject to Indexation.

4.3 Volume Based Service Charges

4.3.1 The Volume Based Service Charges payable by the Authority are set out in Paragraph 2 (*Volume Based Service Charges*) of Annex B (*Service Charges*) to this Schedule 15.

4.3.2 Volume Based Service Charges shall comprise:

- (a) the Service Charges for the provision of the Transport Services as set out in Paragraph 2.1 of Annex B (Service Charges) to this Schedule 15, ("**Transport Service Charges**"); and
- (b) the Service Charges for the provision of the relevant Optional Services as set out in Paragraph 2.2 of Annex B (Service Charges).

4.3.3 The Parties agree that the closure of an Authority Site or a reduction in the Transport Service Charges through business-as-usual activity will be regarded as business-as-usual demand and will not amount to a partial termination under the terms of the Contract. For the avoidance of doubt, subject to Paragraphs 4.3.4 to 4.3.5 below and Schedule 16 (*Payments on Termination*), the Supplier shall not be entitled to receive any payment from the Authority in respect of such closure of an Authority Site or reduction in the number of Site Services.

4.3.3A The Transport Service Charges shall be subject to Indexation.

Minimum Circuit Periods

4.3.4 The Authority shall (unless otherwise agreed in writing by the Authority):

- (a) commit to a minimum initial term of twelve (12) months for each new Access Circuit required for the provision of the Services (the "**Circuit Initial Term**"); and
- (b) give the Supplier at least ninety (90) days' notice to terminate an Access Circuit, provided that where such notice is issued during the Circuit Initial Term, the notice shall not specify a termination date earlier than the expiry of the Circuit Initial Term.

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Minimum Circuit Charges

4.3.5 From the Achievement of Milestone M17 (Transition Complete) the following provisions shall apply to the Access Circuit Charges:

In this Paragraph 4.3.5:

- (a) the “**Access Circuit Charges**” shall be the Transport Service Charges which relate exclusively to the provision of Access Circuits as set out in Paragraph 2.1 of Annex 2 to this Schedule 15, being the DIA Bearer Service Charges, Primary Fixed Broadband Service Charges, Ancillary Fixed Broadband Service Charges but excluding the Mobile Broadband Service Charges;
- (b) the “**Annual Shortfall Payment**” shall, in respect of a Forecast Period, be the multiple of the Annual Shortfall Percentage and the Forecast Annual Circuit Charges calculated on the Circuit Baseline Date for the relevant Forecast Period;
- (c) the “**Annual Shortfall Percentage**” shall, in respect of a Forecast Period, be calculated as the difference between the Annual Volume Variance and 25%;
- (d) the “**Annual Volume Variance**” shall be calculated according to the following formula:

$$\text{Annual Volume Variance \%} = \frac{(F1 - F2)}{F1} \times 100$$

where:

F1 = the Deemed Forecast Annual Circuit Charges calculated on the Circuit Baseline Date for the relevant Forecast Period; and

F2 = the Forecast Annual Circuit Charges calculated on the next occurring Circuit Baseline Date for the next occurring Forecast Period;

- (e) the “**Circuit Baseline Date**” shall be the date of Achievement of Milestone 17 and thereafter, each subsequent anniversary of the Effective Date;
- (f) the “**Deemed Forecast Annual Circuit Charges**” shall, in respect of a Forecast Period, be the greater of:
 - (i) the Forecast Annual Circuit Charges calculated in accordance with 4.3.5(g); or

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (ii) 75% of the Forecast Annual Circuit Charges for the immediately preceding Forecast Period, having regard to Paragraph 4.3.5.1;
 - (g) the “**Forecast Annual Circuit Charges**” shall, in respect of a Forecast Period, be an amount equal to the Access Circuit Charges that would be payable under Paragraph 4.3.2 of this Schedule 15 for all Access Circuits which have been implemented and have not been terminated as at the relevant Circuit Baseline Date for the duration of the relevant Forecast Period; and
 - (h) the “**Forecast Period**” shall be a period of 12 months from the relevant Circuit Baseline Date, subject to 4.3.5.1.
- 4.3.5.1 Notwithstanding 4.3.5(b) and 4.3.5(e) above, where the period between a relevant Circuit Baseline Date and either:
- (a) the next occurring Circuit Baseline Date; or
 - (b) the expiry of the Term,
- is less than 12 months (“**Part Year**”), then:
- (c) the relevant Forecast Period and Forecast Annual Circuit Charges shall be pro-rated to account for the Part Year; and
 - (d) for the purposes of 4.3.5.2 and 4.3.5.3, the next occurring Forecast Period and Forecast Annual Circuit Charges shall also be pro-rated to account for the same Part Year,
- such that there is an equivalent basis for the forecast calculation.
- 4.3.5.2 Subject to Paragraphs 4.3.5.1 and 4.3.5.3 to 4.3.5.5, if at the end of a Forecast Period the Annual Volume Variance is greater than 25% the Supplier shall be entitled to invoice the Authority for the Annual Shortfall Payment.
- 4.3.5.3 For the avoidance of doubt, if at the end of a Forecast Period, the Annual Volume Variance is equal to or less than 25%, then the Supplier shall not be entitled to any payment as a result of such reduction.
- 4.3.5.4 The Supplier shall not be entitled to any payment of the Annual Shortfall Payment if the reduction in the relevant Forecast Annual Circuit Charges is due to:
- (a) this Contract being terminated (in part or in whole) by the Authority pursuant to any provisions in this Contract, except for partial termination for convenience under Clause 31.1A;

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (b) this Contract being terminated (in part or in whole) by the Supplier pursuant to Clause 31.3 (Termination by the Supplier); and/or
 - (c) the expiry of the Term and in no event shall the Authority pay any Annual Shortfall Payment which relate to any period of time after the expiry of this Contract.
- 4.3.5.5 Notwithstanding Paragraphs 4.3.5(b) and 4.3.5.2 above, an Annual Shortfall Payment shall be reduced to the extent that any reduction in the relevant Forecast Annual Circuit Charges is due to:
- (a) the operation of the provisions of Schedule 17 (Benchmarking); and/or
 - (b) any reduction in the price of the Access Circuit Charges that arises other than as a result of the Authority terminating Access Circuits.

For illustrative purposes only, two worked examples of an Annual Shortfall Payment calculation are as follows:

Example 1

F1 calculated on 1 August 2028: £5,000,000

F2 calculated on 1 August 2029: £3,000,000

$$\text{Annual Volume Variance} = \frac{(F1 - F2)}{F1} \times 100 = \frac{£2,000,000}{£5,000,000} \times 100$$

$$= 0.4 \times 100 = \underline{40\%}$$

$$\text{Annual Shortfall Percentage} = 40\% - 25\% = \underline{15\%}$$

$$\text{Annual Shortfall Payment} = 15\% \times £5,000,000 = £750,000^*$$

**Assuming there are no reductions to be applied in accordance with Paragraph 4.3.5.5.*

Example 2

F1 calculated on 1 August 2029: £3,750,000 (*being the Deemed Forecast Annual Circuit Charges 0.75 x £5,000,000*)

F2 calculated on 1 August 2030: £3,000,000

$$\text{Annual Volume Variance} = \frac{(F1 - F2)}{F1} \times 100 = \frac{£750,000}{£3,750,000} \times 100$$

$$= 0.2 \times 100 = 20\%$$

$$\text{Annual Shortfall Percentage} = 20\% - 25\% = \underline{-5\%}$$

Annual Shortfall Payment = Not applicable (*Annual Volume Variance less than 25%*)

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

4.4 Catalogue Item Charges

- 4.4.1 The Product and Services Catalogue contains both chargeable and non-chargeable Catalogue Items. The Catalogue Item Charges in each Service Period shall be the aggregate of the Charges arising in respect of Catalogue Items Consumed by the Authority from the Product and Services Catalogue in that Service Period.
- 4.4.2 The Authority shall be entitled to purchase each Catalogue Item at the price stated in the Product and Services Catalogue set out in Paragraph 3 (Catalogue Item Charges) of Annex B (*Service Charges*) to this Schedule 15.
- 4.4.3 The Supplier shall list prices in the Product and Services Catalogue as either:
- (a) a one-off charge payable by the Authority upon fulfilment of the relevant item;
 - (b) a recurring charge payable by the Authority for the relevant period referred to in the Supplier's Product and Services Catalogue in respect of recurring licence fees or maintenance and support charges; or
 - (c) a discount applicable to a recurring charge payable by the Authority in respect of a Resource Unit.
- 4.4.4 In order to receive payment for Catalogue Items the Authority has ordered and received, the Supplier shall be required to fulfil the Catalogue Item in accordance with (i) the related requirements for that Catalogue Item and (ii) any agreed lead times (as such may be amended or replaced from time to time through the Change Control Process).
- 4.4.5 The Supplier shall submit to the Authority each Service Period a detailed file containing the details of all the amounts which the Supplier considers as due and chargeable for Catalogue Items which have been fulfilled. The Supplier will ensure that such file includes all relevant information extractable from the ITSM Toolset (if applicable), and as a minimum, shall provide the following information:
- (a) task/request reference;
 - (b) date created/requested;
 - (c) date closed/provided;
 - (d) current status;

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (e) delivery location;
 - (f) allocation/business unit/cost centre/entity code;
 - (g) item code;
 - (h) item description; and
 - (i) net amount;
- 4.4.6 The Supplier may only charge single amounts for Catalogue Item Charges verified by and agreed with the Authority. If the Supplier charges an amount for Catalogue Items which has not been approved by the Authority or which is disputed by the Authority, then the Supplier shall immediately credit such amount pending approval by the Authority or resolution of the dispute (as applicable).
- 4.4.7 The Supplier shall submit to the Authority requests for changes to the Service Product and Services Catalogue no more than once per quarter. Requests must be submitted within the following notice periods before the date that the changes to the Supplier's Service Product and Services Catalogue are required to be implemented:
 - (a) with at least fifteen (15) Working Days' notice for modifications to existing Catalogue Items, deletions of existing Catalogue Items or the addition of simple and non-complex Catalogue Items; and
 - (b) with at least thirty (30) Working Days' notice for the addition of new complex Catalogue Items.
- 4.4.8 The Authority will in a timely manner review and raise any queries and then the Supplier will respond and resolve such queries promptly and issue the final request for changes to the Catalogue Items at least ten (10) Working Days before the date that the changes to the Product and Services Catalogue are required to be implemented. Delays in the timely submission of Catalogue Item changes or resolution of Authority queries will result in delayed implementation of changes and payments by the Authority. Any revisions to the pricing of Catalogue Items that are made in accordance with Paragraph 4.4.7 and this Paragraph 4.4.8 shall not be applied retrospectively or back-dated.
- 4.4.9 The Supplier shall ensure when proposing prices to be applicable to each new or revised Catalogue Item to be added to the Product and Services Catalogue that these prices shall be a maximum of the purchase cost (net of any discounts) to the Supplier of the relevant product or service (excluding VAT), plus a maximum uplift (incorporating any handling fee, margin and overhead) not to exceed the Maximum Permitted Profit Margin.

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 4.4.10 Optional charges for support, warranty and/or refresh of a Catalogue Item shall be determined by agreement between the Parties where applicable.
- 4.4.11 If the Authority is able to obtain more favourable commercial terms in respect of any Catalogue Item, the Authority may require the Supplier to enter into more favourable commercial terms as soon as reasonably practicable and in any event no later than 30 days after initial notification to the Supplier by:
- (a) requiring the Supplier to replace its existing commercial terms with the more favourable commercial terms obtained by the Authority in respect of the relevant item; or
 - (b) subject to Paragraph 4.4.13, entering into a direct agreement with the supplier of that Catalogue Item in respect of the relevant Catalogue Item;
- provided that if the Catalogue Item is replaced in order to obtain the more favourable commercial terms, any replacement Catalogue Item has the same or substantially similar specification as the original Catalogue Item.
- 4.4.12 If the Authority exercises either of its options pursuant to Paragraph 4.4.11, then the price for that Catalogue Item shall be reduced by an amount that is agreed in accordance with the Change Control Procedure, and any Charges based on those Catalogue Items shall be reduced accordingly provided that the reduction shall not be applied retrospectively or back-dated.
- 4.4.13 The Authority's right to enter into a direct agreement for the supply of the relevant items is subject to:
- (a) the Authority making the relevant item available to the Supplier where this is necessary for the Supplier to provide the Services; and
 - (b) any reduction in the Charges taking into account any unavoidable costs payable by the Supplier in respect of the substituted item, including in respect of any licence fees or early termination charges.
- 4.4.14 The Supplier shall not be entitled to add any costs, other than those listed at Paragraph 4.4.9 above, to the charges for Catalogue Items.
- 4.4.15 The Supplier shall identify any relevant lead times for the fulfilment of each Catalogue Item in the Product and Services Catalogue, such lead times to commence upon receipt of a Service Request for the Catalogue Item from the Authority.

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

4.4.16 If the Authority purchases assets, materials, software and equipment from the Product and Services Catalogue, then these shall be deemed to be Authority Assets.

4.4.17 For the avoidance of doubt, the Catalogue Item Charges shall not be subject to Indexation.

5 CALCULATION OF MONTHLY SERVICE CHARGES

5.1 Following the first Operational Service Commencement Date, Service Charges shall be invoiced by the Supplier for each Service Period in arrears in accordance with the requirements of Part E (*Invoicing and Payment Terms*) of this Schedule 15.

5.2 If a Service Charge:

5.2.1 commences on a day other than the first day of a month; and/or

5.2.2 ends on a day other than the last day of a month,

the Service Charge for the relevant Service Period shall be pro-rated based on the proportion which the number of days in the month for which the Service is provided bears to the total number of days in that month.

5.3 The Service Charges for each Service Period ("**Monthly Service Charges**") shall be the aggregate of:

5.3.1 the Fixed Service Charges for the relevant Service Period; and

5.3.2 the Volume Based Service Charges for the relevant Service Period; and

5.3.3 the Catalogue Item Charges for the relevant Service Period.

5.4 The Supplier acknowledges and agrees that the Authority gives no warranty or representation as to:

5.4.1 the volume of Operational Services; and/or

5.4.2 the total Service Charges.

Service Credits

5.5 Any Service Credits that accrue during a Service Period shall be deducted from the Monthly Service Charges payable in respect of the next following Service Period. An invoice for a Service Charge shall not be payable by the Authority unless all adjustments (including Service Credits) relating to the Service Charges for the immediately preceding Service Period have been agreed.

5.6 Service Credits shall be applied against the Service Charges in accordance with Paragraph 3 of Part C (*Adjustments to the Charges*) of this Schedule 15.

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

6 TIME AND MATERIAL CHARGES

6.1 Where the Parties agree in writing that a particular Charge is to be calculated by reference to a Time and Materials pricing mechanism (e.g. pursuant to a Contract Change):

6.1.1 the day rates set out in the table in Annex C (*Rate Card*) to this Schedule 15 shall be used to calculate the relevant Charges, provided that the Supplier (or its Sub-contractor) shall:

- (a) not be entitled to include any uplift for risks or contingencies within its day rates;
- (b) not be paid any Charges to the extent that they would otherwise exceed any cap on such Charges agreed in writing by the Parties unless the Supplier has obtained the Authority's prior written consent. The Supplier shall monitor the amount of each Charge incurred in relation to the relevant cap and notify the Authority immediately in the event of any risk that the cap may be exceeded and the Authority shall instruct the Supplier on how to proceed;
- (c) only be entitled to be paid Charges that have been properly and reasonably incurred, taking into account the Supplier's obligation to deliver the Services in a proportionate and efficient manner;

6.1.2 the Supplier shall keep records of hours properly worked by Supplier Personnel (in the form of timesheets) and expenses incurred and submit a summary of the relevant records with each invoice. If the Authority requests copies of such records, the Supplier shall make them available to the Authority within ten (10) Working Days of the Authority request; and

6.1.3 time and materials will be charged to the nearest hour and will be rounded to the nearest hour.

6.2 The Supplier shall be entitled to Index the rates set out in Table 12 in Annex C (*Rate Card*) to this Schedule 15 in accordance with Paragraph 5 of Part C (*Adjustments to the Charges and Risk Register*) of this Schedule 15.

7 REIMBURSABLE EXPENSES

7.1 The Charges (including the Milestone Payments, Fixed Service Charges, Volume Based Service Charges, Catalogue Item Charges, Excess Construction Charges and Rate Card) are all inclusive of costs and expenses relating to the Deliverables, the Services and/or the Supplier's performance of its obligations under this Contract and no further amounts shall be payable by the Authority to the Supplier in respect of such performance, including in respect of matters such as:

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 7.1.1 any incidental expenses that the Supplier incurs, including travel, subsistence and lodging, document and report reproduction, shipping, desktop and office equipment costs required by the Supplier Personnel, including network or data interchange costs or other telecommunications charges; or
 - 7.1.2 any amount for any Services provided or costs incurred by the Supplier prior to the Commencement Date.
- 7.2 The Supplier shall only be entitled to be reimbursed by the Authority for Reimbursable Expenses (in addition to being paid the relevant Charges) if the Authority has approved such expenses in writing prior to the expenses being incurred and provided that such Reimbursable Expenses are supported by Supporting Documentation.

8 EXCESS CONSTRUCTION CHARGES

- 8.1 **“Excess Construction Charge(s)”** shall mean additional infrastructure and construction costs that have been identified following a site survey at an Authority Site that are required and are necessary to enable the provision of the required network connectivity at such Authority Site and are in addition to the normal/standard costs to enable such connectivity for the Authority Site.
- 8.2 Where, having complied with its obligations in Paragraphs 7.1.1.6 and 7.1.1.7 of the Transition Requirements, the Supplier incurs any Excess Construction Charge(s), then subject to:
 - 8.2.1 the Authority being satisfied that the Supplier has provided sufficient evidence of the Excess Construction Charges being required and has taken reasonable steps to mitigate and minimise Excess Construction Charge(s);
 - 8.2.2 the Authority having given its prior written approval to the Supplier incurring the relevant Excess Construction Charge(s); and
 - 8.2.3 the Supplier providing Supporting Documentation for the relevant Excess Construction Charge(s),

the Supplier may invoice the Authority for the amount of the relevant Excess Construction Charge(s), which will be paid by the Authority on a pass-through basis, with no mark-up added to the Excess Construction Charge(s) by the Supplier.

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Part B: Project Charges**1. INTRODUCTION**

- 1.1 If the Parties agree that the Supplier shall provide a Project, then the Charges payable by the Authority for such Project shall be payable on the basis of the charging mechanism set out in the relevant Project Work Order or agreed in accordance with the Change Control Procedure. Wherever possible, a Project Work Order should use Catalogue Items if relevant to the Project.
- 1.2 The Project Charges for a Project shall be calculated on the basis of either:
- 1.2.1 a fixed price, payable in one or more Milestone Payments in accordance with Paragraph 2 (*Milestone Payments*) of this Part B; or
 - 1.2.2 a Guaranteed Maximum Price with Target Cost mechanism, payable in accordance with Paragraph 3 of this Part B; or
 - 1.2.3 Time and Material Charges, in which event Paragraph 6 (*Time and Materials Charges*) of Part A (*Pricing*) of this Schedule 15 will apply; or
 - 1.2.4 Catalogue Item Charges, in which event Paragraph 4.4 (*Catalogue Items*) of Part A (*Pricing*) of this Schedule 15 will apply.

2. Milestone Payments

- 2.1 The Parties may specify Milestone Payments as the charging basis for part or all of a Project.
- 2.2 Project Work Orders that specify Charges payable on the basis of Milestone Payments shall set out the details of each Milestone Payment, including the Milestone Date, amount payable and value of any Milestone Retention and/or Delay Payment (if applicable).
- 2.3 Subject to paragraphs 2.4 to 2.6 below, the Supplier shall be entitled to deliver an invoice to the Authority in respect of each Milestone Payment (less any applicable Milestone Retention):
- 2.3.1 on the issue by the Authority of a Milestone Achievement Certificate in accordance with Schedule 14 (*Testing Procedures*); or
 - 2.3.2 on the Supplier Achieving and evidencing the agreed Test Success Criteria to the Authority's reasonable satisfaction as set out in a Project Work Order,
- for the Milestone associated with that Milestone Payment.
- 2.4 The circumstances in which a Milestone shall be considered to have been Achieved are set out in the relevant Project Work Order. Payment shall be

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

made to the Supplier in accordance with Part E (*Invoicing and Payment Terms*) of this Schedule 15.

2.5 The circumstances in which a Milestone Retention shall be released shall be set out in in the relevant Project Work Order.

2.6 Unless otherwise agreed in the Project Work Order, Milestone Payments shall constitute full consideration for the Project and shall be fully inclusive of all costs and expenses incurred in performance of the applicable Project.

3. GUARANTEED MAXIMUM PRICE WITH TARGET COST PRICING MECHANISM

3.1 Where a Project Work Order states, or it is agreed pursuant to the Change Control Procedure, that the Project Charges are to be calculated by reference to a Guaranteed Maximum Price with Target Cost pricing mechanism, then the following payment process shall apply.

3.2 If the Incurred Costs relating to a Milestone are lower than the Target Cost for that Milestone, the difference between the Incurred Costs and the Target Cost shall be shared equally between the Authority and the Supplier (resulting in the Supplier receiving a higher Supplier Profit Margin in relation to that Milestone), and the Milestone Payment shall be calculated as follows:

$$\text{Milestone Payment} = \text{TP} - ((\text{TC} - \text{IC})/2)$$

where:

TP is the Target Price for the relevant Milestone;

TC is the Target Cost for the relevant Milestone; and

IC is the Incurred Costs relating to the relevant Milestone.

3.3 If the Incurred Costs relating to a Milestone are greater than the Target Cost for that Milestone, the difference between the Incurred Costs and the Target Cost shall be borne equally between the Authority and the Supplier (resulting in the Supplier receiving a lower Supplier Profit Margin in relation to that Milestone), provided that the maximum Milestone Payment payable by the Authority for the relevant Milestone shall not exceed an amount equal to the guaranteed maximum price for that Milestone as set out in the relevant Project Work Order (the "**Guaranteed Maximum Price**") Represented numerically:

(a) if:

(i) $\text{IC} > \text{TC}$; and

(ii) $\text{TP} + ((\text{IC} - \text{TC})/2) < \text{GMP}$,

then Milestone Payment = $\text{TP} + ((\text{IC} - \text{TC})/2)$; or

(b) if:

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (i) $IC > TC$; and
 - (ii) $TP + ((IC - TC)/2) \geq GMP$,
- then Milestone Payment = GMP

where:

IC is the Incurred Costs relating to the relevant Milestone;

TC is the Target Cost for the relevant Milestone;

TP is the Target Price for the relevant Milestone; and

GMP is $TP * 1.1$, being the Guaranteed Maximum Price for the relevant Milestone.

3.4 Upon the issue of an Achievement Certificate for the Milestone, the Supplier may invoice the Authority for the Target Price for the relevant Milestone, less the Milestone Retention calculated using such Target Price.

3.5 No later than 60 Working Days after the invoice referred to in Paragraph 3.4 has been issued, the Supplier shall:

3.5.1 submit to the Authority a report setting out the Incurred Costs and actual Milestone Payment for the Milestone;

3.5.2 issue to the Authority an invoice or credit note for the difference between the actual Milestone Payment payable and the Target Price invoiced for the Milestone (in each case, after deducting the applicable Milestone Retention);

3.5.3 where a credit note is to be issued to the Authority pursuant to Paragraph 3.5.2 repay to the Authority a sum equal to such difference as a debt within 10 Working Days of issue of the credit note; and

3.5.4 issue a Certificate of Costs with Supporting Documentation, which shall exclude any accruals, prepayments and provisions.

Milestone Groups

3.6 Where Milestones are stated in a Project Work Order or agreed in accordance with the Change Control Procedure to constitute a group of Milestones (a "**Milestone Group**") and the Milestone Payments relating to the Milestones in that Milestone Group are each to be calculated by reference to a Guaranteed Maximum Price with Target Cost pricing mechanism, then the following payment process shall apply:

3.6.1 in respect of each Milestone within the Milestone Group, the Supplier may invoice the Authority for the Target Price for the

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

relevant Milestone, less the Milestone Retention calculated using such Target Price, upon the issue of the associated Milestone Achievement Certificate; and

- 3.6.2 no later than 60 Working Days after the issue of the invoice for the final Milestone Payment relating to the Milestone Group, the Supplier shall:
- (a) submit to the Authority a report setting out the Incurred Costs and actual Milestone Payments for the Milestone Group;
 - (b) issue to the Authority an invoice or credit note for the difference between the aggregate of the actual Milestone Payments payable and Target Prices invoiced for Milestones in the Milestone Group (in each case, after deducting all Milestone Retentions relating to that Milestone Group);
 - (c) where a credit note is to be issued to the Authority pursuant to Paragraph 3.6.2(b) repay to the Authority a sum equal to such difference as a debt within 10 Working Days of issue of the credit note; and
 - (d) issue a Certificate of Costs with Supporting Documentation, which shall exclude any accruals, prepayments and provisions.
- 3.7 If the Supplier does not repay any such sum as is referred to in Paragraph 3.5.3 or 3.6.2(b) within 10 Working Days of issue of the relevant credit note, it shall repay such sum together with interest on such sum at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from (and including) the due date up to (but excluding) the date of actual payment, whether before or after judgment.
- 3.8 Following the issue of a Certificate of Costs in accordance with Paragraph 3.5.3 or 3.6.2(c), the Supplier shall not be entitled to invoice the Authority for any additional Charges relating to the Milestone or Milestone Group (as applicable) save as provided in Paragraph 3.5.
- Release of Milestone Retentions**
- 3.9 The circumstances in which a Milestone Retention shall be released shall be set out in in the relevant Project Work Order or Change Authorisation Note.

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Part C: Adjustments to the Charges and Risk Register**1 DELAY PAYMENTS**

1.1 If a Key Milestone has not been Achieved on or before the relevant Milestone Date, the Supplier shall notify the Authority and shall pay a Delay Payment to the Authority in respect of that Key Milestone. Delay Payments shall accrue:

(a) at the daily rate (the “**Delay Payment Rate**”) set out in column 10 (*Amount of Delay Payments*) of Table 1 in Annex A (*Key Milestones, Payment Milestones, Milestone Payments and Delay Payments*) to this Schedule 15 for the relevant Key Milestone;

(b) from (but excluding) the relevant Milestone Date to (and including) the earlier of:

(i) the date on which the Key Milestone is Achieved; and

(ii) the expiry of the Delay Deduction Period; and

(c) on a daily basis, with any part day’s Delay counting as a day,

provided that the Supplier’s aggregate liability in respect of Delay Payments shall be subject to the Delay Payment Cap.

1.2 In the event the circumstances described in Paragraph 1.1 apply, then following the earlier of (i) the Authority being notified by the Supplier pursuant to Paragraph 1.1 that a Key Milestone has not been Achieved and (ii) the relevant Milestone Date, the Supplier shall issue a credit note to the Authority in respect of the relevant amount.

1.3 The Parties agree that Delay Payments calculated in accordance with the applicable Delay Payment Rates are in each case reflective of a genuine pre-estimate of the Losses which the Authority will incur as a result of any failure by the Supplier to Achieve the relevant Key Milestone by the Milestone Date. Delay Payment Rates are stated exclusive of VAT.

1.4 The Delay Payment in respect of a Key Milestone (net of any payment made in respect of that Key Milestone pursuant to Paragraph 1.2) shall be shown as a deduction from the amount due from the Authority to the Supplier in the next invoice due to be issued by the Supplier after the date on which the relevant Key Milestone is Achieved or the expiry of the Delay Deduction Period (as the case may be). If the relevant Key Milestone is not Achieved by the expiry of the Delay Deduction Period and no invoice is due to be issued by the Supplier within 10 Working Days of expiry of the Delay Deduction Period, then the Supplier shall within 10 Working Days of expiry of the Delay Deduction Period:

(a) issue a credit note to the Authority in respect of the total amount of the Delay Payment in respect of the Key Milestone (net of any payment made in respect of the Key Milestone pursuant to Paragraph 1.2); and

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (b) pay to the Authority as a debt a sum equal to the total amount of the Delay Payment in respect of the Key Milestone together with interest on such amount at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from (and including) the due date up to (but excluding) the date of actual payment, whether before or after judgment.

2 PAYMENTS FOR DELAYS DUE TO AUTHORITY CAUSE

2.1 If the Supplier is entitled in accordance with Clause 29.1(iii)(D) (*Authority Cause*) to compensation for failure to Achieve a Milestone by its Milestone Date, then, subject always to Clause 23 (*Limitations on Liability*), such compensation shall be determined in accordance with the following principles:

- (a) the compensation shall reimburse the Supplier for additional Costs incurred by the Supplier that the Supplier:
 - (i) can demonstrate it has incurred solely and directly as a result of the Authority Cause; and
 - (ii) is, has been, or will be unable to mitigate, having complied with its obligations under Clause 29.1 (*Authority Cause*)

together with an amount equal to the Anticipated Contract Life Profit Margin thereon;

- (b) the compensation shall not operate so as to put the Supplier in a better position than it would have been in but for the occurrence of the Authority Cause;
- (c) where the Milestone Payment for the relevant Milestone is to be calculated by reference to the Guaranteed Maximum Price with Target Cost pricing mechanism, then:
 - (i) the Target Price for the Milestone shall be increased in accordance with the following formula:

$$NTP = TP + (AC \times 1.x)$$

where:

NTP is the revised Target Price for the relevant Milestone;

TP is the original Target Price for the relevant Milestone;

AC is an amount equal to any additional Costs incurred by the Supplier in Achieving the Milestone to the extent that the Supplier can

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

demonstrate that such additional Costs were caused by the Authority Cause; and

X is the Supplier Profit Margin that the Supplier would have received in respect of the relevant Milestone on the basis of the unadjusted Target Cost and unadjusted Target Price for that Milestone, as set out in the relevant Project Work Order, expressed as a decimal; and

(ii) the Guaranteed Maximum Price shall be increased to an amount equal to 110% of the Target Price as adjusted pursuant to Paragraph 2.1(c)(i);

(d) where the relevant Milestone Payment is to be calculated based upon a Fixed Price or a Firm Price pricing mechanism, the compensation shall include such amount as is appropriate to maintain the Supplier Profit Margin and shall take into account any Milestone Retention(s) which would (but for the relevant Authority Cause) have been released on the Achievement of the relevant Milestone; and

(e) where the Milestone Payment includes any Charges which are capped, then to the extent that the compensation agreed pursuant to this Paragraph 2 results in the Authority paying additional Time and Materials Charges for resources or effort which the Supplier demonstrates are required as a result of the Authority Cause, such additional Time and Materials Charges shall be disregarded for the purposes of calculating the relevant cap.

2.2 The Supplier shall provide the Authority with any information the Authority may require in order to assess the validity of the Supplier's claim to compensation.

3 SERVICE CREDITS

3.1 Service Credits shall be calculated in accordance with:

3.1.1 Paragraphs 3.5 to 3.10 of this Part C; and

3.1.2 by reference to the number of applicable Service Points accrued in any one Service Period pursuant to the provisions of Schedule 3 (*Performance Levels*).

3.2 The liability of the Supplier in respect of Service Credits shall be subject to Clause 23.4(c) (Financial and other Limits) provided that, for the avoidance of doubt, the operation of the Service Credit Cap shall not affect the continued accrual of Service Points in excess of such financial limit in accordance with the provisions of Schedule 3 (*Performance Levels*).

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

3.3 Service Credits are a reduction of the Service Charges payable in respect of the relevant Services to reflect the reduced value of the Services received and are stated exclusive of VAT.

3.4 Service Credits shall be shown as a deduction from the amount due from the Authority to the Supplier in the invoice for the Service Period immediately succeeding the Service Period to which they relate.

Availability: Gateway Services (KPI-01b)

3.5 The Service Credit due in respect of KPI-01b for the Gateway Services in each Service Period shall be calculated in accordance with the following formula:

$$SC = A \times B \times C$$

where:

SC is the Service Credit due for the Service Period; and

A is the applicable Service Points that have accrued in the Service Period in accordance with Part A of Annex 1 (*Key Performance Indicators and Subsidiary Performance Indicators*) to Schedule 3 (*Performance Levels*); and

B is the applicable percentage deduction 0.01%; and

C is the sum of the Gateway Service Charges for the Service Period in accordance with Paragraph 1 (*Fixed Service Charges*) of Annex B (*Service Charges*) to this Schedule.

Availability: WAN Connectivity (KPI-01a)

3.6 The Service Credit due in respect of KPI 01a for each applicable Authority Site in each Service Period shall be calculated in accordance with the following formula:

$$SC = A \times B$$

where:

SC is the Service Credit due for the KPI in the Service Period; and

A is the applicable Service Points that have accrued in the Service Period as defined in Part A of Annex 1 (*Key Performance Indicators and Subsidiary Performance Indicators*) to Schedule 3 (*Performance Levels*)); and

B is the applicable Service Credit Point Value, calculated for each Authority Site in accordance with Paragraph 3.7 below.

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Service Credit Point Value

- 3.7 The Service Credit Point Value for KPI 01a is calculated for each Authority Site in accordance with the following formula:

$$\text{Service Credit Point Value} = (A \times B) / C$$

where:

- A** is the sum of the Transport Service Charges for the Service Period for the relevant Authority Site in accordance with the Authority Site Specification and Paragraph 2 (*Volume Based Service Charges*) of Annex B (*Service Charges*) to this Schedule; and
- B** is the applicable “At Risk Percentage” being:
- (i) 80% for a Gold Site;
 - (ii) 65% for a Silver Site; or
 - (iii) 50% for a Bronze Site;
- and
- C** is the applicable number of “Service Credit Increments” calculated in accordance with Paragraph 3.8 below.

Service Credit Increments

- 3.8 The Service Credit Increments for KPI-01a are calculated for each Authority Site in accordance with the following formula:

$$\text{Service Credit Increments} = \frac{A - B}{C}$$

where:

- A** is the applicable Target Performance Level for the relevant Authority Site for KPI-01a; and
- B** is the applicable KPI Service Threshold for the relevant Authority Site for KPI-01a; and
- C** is 0.01%.

Service Availability Performance Levels

- 3.9 The Target Performance Levels and KPI Service Thresholds for each applicable Site Type for KPI-01a are set out in Paragraph 2.4 of Part B of Annex 1 (*Key Performance Indicators and Subsidiary Performance Indicators*) to Schedule 3 (*Performance Levels*). The Target Performance Level and KPI Service Threshold for the Gateway Services for KPI-01b are set out in Paragraph 1.1 of Part A of Annex 1 (*Key Performance Indicators and Subsidiary Performance Indicators*) to Schedule 3 (*Performance Levels*).

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Operational KPIs (KPI-02 to KPI-08)

- 3.10 The Service Credit due in respect of each other Operational KPI (KPIs 02 to 08) in each Service Period shall be calculated in accordance with the following formula:

$$SC = A \times B \times C$$

where:

- SC is the Service Credit due for the Service Period; and
 - A is the applicable Service Points that have accrued in the Service Period in accordance with Annex 1 (*Key Performance Indicators and Subsidiary Performance Indicators*) to Schedule 3 (*Performance Levels*); and
 - B is the applicable percentage deduction, being either:
 - (i) 0.01% in respect of KPI-02 to KPI-05; or
 - (ii) 0.1% in respect of KPI-06 to KPI-08; and
 - C is the applicable service charges which are calculated as the aggregate of the Fixed Service Charges and the Volume Based Charges for the Service Period.
- 3.11 Illustrative examples of Service Credit calculations are set out in Annex H (*Illustration of Service Points Accrual and Service Credits*) to this Schedule 15.

4 CHANGES TO CHARGES

- 4.1 Any Changes to the Charges shall be developed and agreed by the Parties in accordance with Schedule 22 (*Change Control Procedure*) and on the basis that the Supplier Profit Margin on such Charges shall:
- (a) be no greater than that applying to Charges using the same pricing mechanism as at the Effective Date (as set out in the Contract Inception Report); and
 - (b) in no event exceed the Maximum Permitted Profit Margin.
- 4.2 The Authority may request that any Impact Assessment presents Charges without Indexation for the purposes of comparison.

5 INDEXATION

- 5.1 Any amounts or sums in this Contract which are expressed to be “subject to Indexation” shall be adjusted in accordance with the provisions of this Paragraph 5 to reflect the effects of inflation.
- 5.2 Where Indexation applies, the relevant adjustment shall be:
- (a) applied on the first day of the second April following the Effective Date and on the first day of April in each subsequent year (each such date an “**adjustment date**”); and

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (b) for rate card charges set out in Annex C (*Rate Card*), determined by multiplying the relevant amount or sum by the percentage increase or changes in the Average Weekly Earnings – regular pay for the 12 months ended on the 31 January immediately preceding the relevant adjustment date; and
 - (c) for all other Charges stated to be subject to Indexation, determined by multiplying the relevant amount or sum by the percentage increase or changes in the Consumer Price Index published for the 12 months ended on the 31 January immediately preceding the relevant adjustment date.
- 5.3 Except as set out in this Paragraph 5, neither the Charges nor any other costs, expenses, fees or charges shall be adjusted to take account of any inflation, change to exchange rate, change to interest rate or any other factor or element which might otherwise increase the cost to the Supplier or Sub-contractors of the performance of their obligations.

6 ALLOWABLE ASSUMPTIONS

- 6.1 The Supplier shall determine whether each Allowable Assumption is accurate within its Verification Period.
- 6.2 During each Verification Period, the Authority shall provide the Supplier with reasonable assistance and access to information within its possession or reasonable control and which the Authority deems is relevant to the Allowable Assumption being verified.
- 6.3 Within 10 Working Days of the end of each Verification Period, the Supplier shall provide the Authority with a written report setting out the results of the Supplier's verification activity for the relevant Allowable Assumption, including whether the Allowable Assumption is accurate or whether the Implementation Plan and/or the Contract Inception Report require adjustment.
- 6.4 Each Allowable Assumption shall be deemed accurate unless adjusting for the relevant Allowable Assumption has an impact:
- (a) on the Financial Model greater than the associated "Trigger for Invocation" for the relevant Allowable Assumption; or
 - (b) on the Implementation Plan which would require adjustment under the Change Control Procedure, as identified in the "Impact on the Implementation Plan" for the relevant Allowable Assumption,
- in which case Paragraph 6.5 shall apply.
- 6.5 Where the Parties agree that an Allowable Assumption is not accurate and the Financial Model and/or Implementation Plan require adjusting:
- (a) the Supplier shall take all reasonable steps to mitigate the impact of the Allowable Assumption on the Financial Model and/or the Implementation Plan;

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (b) the Supplier may (subject to Paragraph 6.5(c)) propose a Change to take account of the impact of the adjustment of the Allowable Assumption and such Change Request shall be considered in accordance with the Change Control Procedure; and
- (c) where the Supplier proposes a Change to the Charges under Paragraph 6.5(b), the Change Request shall reflect the requirements of the table in Annex F (*Allowable Assumptions*), including the requirement that any proposed adjustment to the Charges shall not exceed the maximum impact on the relevant Charges as specified in column 7 of the table in Annex F (*Allowable Assumptions*).

7 RISK REGISTER

- 7.1 The Parties shall review the Risk Register set out in Annex E (*Risk Register*) from time to time and as otherwise required for the purposes of Schedule 21 (*Governance*).

8 TRUE UP MECHANISM FOR TUPE COSTS

- 8.1 The Authority acknowledges that the Supplier has based its pricing as set out in the 'Bidder Baseline Charges Summary' worksheet of the Financial Response Template (FRT) on the information set out in the 'TUPE' worksheet of the FRT ("**the Initial TUPE Information**").
- 8.2 The Authority shall allow, after a Relevant Transfer from the Former Supplier and/or its sub-contractors, a reconciliation exercise to be conducted by the Supplier on the Preceding Supplier's TUPE information and any TUPE information supplied by the Preceding Supplier's sub-contractor(s) during the procurement.
- 8.3 If awarded the Contract, after a Relevant Transfer, the Supplier will compare the Initial TUPE Information with the actual employment information that the Supplier receives upon the Relevant Transfer ("**the Final TUPE Information**").
- 8.4 The Supplier must undertake the comparison exercise referred to in Paragraph 8.3 immediately after the Relevant Transfer has taken place and shall complete this exercise within 60 Working Days of the Relevant Transfer.
- 8.5 The Supplier is only permitted to undertake this exercise once in respect of each Relevant Transfer, from the Former Supplier and/or its sub-contractors, which takes place during the Contract Period (or, if sooner, until the cap referred to in Paragraph 8.8 below has been reached).
- 8.6 Within 10 Working Days of completion of the comparison exercise, the Supplier shall send a report ("**the Reconciliation Report**") to the Authority detailing the differences between the Initial TUPE Information and the Final TUPE Information.

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 8.7 Subject to Paragraph 8.8, the Parties shall then agree in accordance with the Change Control Procedure any corresponding adjustment (up or down) to the Charges to reflect the differences identified in the Reconciliation Report. The Supplier shall justify any claims for an increase in the Charges by demonstrating to the Authority's reasonable satisfaction the impact that any increased employee numbers and/or related costs detailed in the Final TUPE Information (as compared to those assessed by reference to the Initial TUPE Information) have on the Charges.
- 8.8 The total value of any increase to the Charges will be capped at a maximum of 10% (ten per cent) of the Supplier's 'Total TUPE Costs' as set out in the worksheet entitled 'TUPE' in the FRT.

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Part D: Excessive Supplier Profit Margin**1 LIMIT ON SUPPLIER PROFIT MARGIN**

- 1.1 The Supplier acknowledges that the Achieved Profit Margin applicable over the Term shall not exceed the Maximum Permitted Profit Margin.
- 1.2 The Supplier shall include in each Annual Contract Report the Achieved Profit Margin as at the end of the Contract Year to which the Annual Contract Report is made up and the provisions of Paragraph 2 of Part B of Schedule 19 (*Financial Reports and Audit Rights*) shall apply to the approval of the Annual Contract Report.

2 ADJUSTMENT TO THE CHARGES IN THE EVENT OF EXCESS SUPPLIER PROFIT

- 2.1 If an Annual Contract Report demonstrates (or it is otherwise determined pursuant to Paragraph 2 Part B of Schedule 19 (*Financial Reports and Audit Rights*)) that the Achieved Profit Margin as at the end of the Contract Year to which the Annual Contract Report is made up exceeds the Maximum Permitted Profit Margin:
- (a) the Supplier shall, within 5 Working Days of delivery to the Authority of the Annual Contract Report, propose such adjustments to the Charges as will ensure that the Achieved Profit Margin both over the Contract Year to which the next Annual Contract Report will relate and over the Term will not exceed the Maximum Permitted Profit Margin;
 - (b) the Authority (acting reasonably) may agree or reject the proposed adjustments;
 - (c) if the Authority rejects the proposed adjustments, it shall give reasons and the Supplier shall propose revised adjustments within 10 Working Days of receiving those reasons; and
 - (d) if the Parties cannot agree such revised adjustments and the Authority terminates this Contract by issuing a Termination Notice to the Supplier pursuant to Clause 31.1(a) (*Termination by the Authority*), then for the purpose of calculating any Compensation Payment due to the Supplier, the Termination Notice shall be deemed to have been served as at the date of receipt by the Authority of the relevant Annual Contract Report.
- 2.2 Pending agreement of a proposed adjustment to the Charges pursuant to this Part D, the Charges then in force shall continue to apply. Once the adjustments to the Charges are agreed in accordance with Paragraph 2.1, the Parties shall document the adjustment in a Change Authorisation Note and the adjusted Charges shall apply with effect from the first day of the Service Period that immediately follows the Service Period in which the Change

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Authorisation Note is executed on such other date as is specified in the Change Authorisation Note.

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Part E: Invoicing and Payment Terms**1 SUPPLIER INVOICES**

- 1.1 The Authority shall accept for processing any electronic invoice that complies with the European Standard, provided that it is valid and undisputed.
- 1.2 If the Supplier proposes to submit for payment an invoice that does not comply with the European standard the Supplier shall:
- (a) comply with the requirements of the Authority's e-invoicing system;
 - (b) prepare and provide to the Authority for approval of the format a template invoice within 10 Working Days of the Effective Date which shall include, as a minimum the details set out in Paragraph 1.3 together with such other information as the Authority may reasonably require to assess whether the Charges that will be detailed therein are properly payable; and
 - (c) make such amendments as may be reasonably required by the Authority if the template invoice outlined in (b) is not approved by the Authority.
- 1.3 The Supplier shall ensure that each invoice is submitted in the correct format for the Authority's e-invoicing system, or that it contains the following information:
- (a) the date of the invoice;
 - (b) a unique invoice number;
 - (c) the Service Period or other period(s) to which the relevant Charge(s) relate;
 - (d) the correct reference for this Contract;
 - (e) the reference number of the purchase order to which it relates (if any);
 - (f) the dates between which the Services subject of each of the Charges detailed on the invoice were performed;
 - (g) a description of the Services;
 - (h) the pricing mechanism used to calculate the Charges (such as Guaranteed Maximum Price with Target Cost, Fixed Price, Time and Materials);
 - (i) any payments due in respect of Achievement of a Milestone, including the Milestone Achievement Certificate number for each relevant Milestone;
 - (j) the total Charges gross and net of any applicable deductions and, separately, the amount of any Reimbursable Expenses properly

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

chargeable to the Authority under the terms of this Contract, and, separately, any VAT or other sales tax payable in respect of each of the same;

- (k) details of any Service Credits or Delay Payments or similar deductions that shall apply to the Charges detailed on the invoice;
 - (l) reference to any reports required by the Authority in respect of the Services to which the Charges detailed on the invoice relate (or in the case of reports issued by the Supplier for validation by the Authority, then to any such reports as are validated by the Authority in respect of the Services);
 - (m) a contact name and telephone number of a responsible person in the Supplier's finance department in the event of administrative queries;
 - (n) the banking details for payment to the Supplier via electronic transfer of funds (i.e. name and address of bank, sort code, account name and number);
 - (o) applicable Authority cost centre and entity codes; and
 - (p) where the Services have been structured into separate Service lines, the information at (a) to (n) of this Paragraph 1.3 shall be broken down in each invoice per Service line.
- 1.4 The Supplier shall invoice the Authority in respect of Services in accordance with the requirements of this Part E. Each invoice will only be paid if the amount matches the amount agreed through the Payment Planner process as detailed in Paragraph 2 (*Payment Planner*) of this Part E.
- 1.5 Each invoice shall at all times be accompanied by Supporting Documentation. Any assessment by the Authority as to what constitutes Supporting Documentation shall not be conclusive and the Supplier undertakes to provide to the Authority any other documentation reasonably required by the Authority from time to time to substantiate an invoice.
- 1.6 The Supplier shall submit all invoices and Supporting Documentation through the Authority's electronic system or if that is not possible to:
- SSCL – MoJ
PO Box 743,
Newport, NP10 8FZ
APinvoices-MOJ-U@gov.sscl.com
- with a copy (again including any Supporting Documentation) to such other person and at such place as the Authority may notify to the Supplier from time to time.
- 1.7 All Supplier invoices shall be expressed in sterling, or such other currency as shall be permitted by the Authority in writing.

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 1.8 The Authority shall regard an invoice as valid only if it complies with the provisions of this Part E. Where any invoice does not conform to the Authority's requirements set out in this Part E, the Authority shall promptly return the disputed invoice to the Supplier and the Supplier shall promptly issue a replacement invoice which shall comply with such requirements.
- 1.9 If the Authority fails to consider and verify an invoice in accordance with Paragraphs 1.4 and 1.8, the invoice shall be regarded as valid and undisputed for the purpose of Paragraph 3.1 of this Part E after a reasonable time has passed.

2 PAYMENT PLANNER

- 2.1 Except for Catalogue Item Charges, the Supplier shall provide and maintain a Payment Planner in the format set out in Annex G (*Payment Planner*) to this Schedule 15, detailing all anticipated Charges.
- 2.2 The Supplier shall ensure that the Payment Planner is consistent with the Financial Model and is kept up to date on at least a monthly basis.
- 2.3 The Supplier shall submit a single draft Payment Planner to the Authority no more than ten (10) Working Days from the start of each month.
- 2.4 The draft Payment Planner shall at all times be accompanied by sufficient information to enable the Authority to reasonably assess whether the Charges detailed therein are properly payable. Any such assessment by the Authority shall not be conclusive. The Supplier undertakes to provide to the Authority any other documentation reasonably required by the Authority from time to time to substantiate an invoice.
- 2.5 The Payment Planner shall be based on volume information which has been verified in accordance with the Services Description.
- 2.6 For the avoidance of doubt, the Charges appearing in the Payment Planner are Charges which are scheduled for payment in the month to which the Payment Planner relates, not the month in which the Services to which the Charges relate are performed. For example, if a Milestone Achievement Certificate has not been issued by the Authority by the time the draft Payment Planner is submitted, then such amounts should not be included under the current month's Charges in the Payment Planner. They should instead be deferred until the Milestone Achievement Certificate has been issued but should still be included in the Payment Planner (under a future month), so that the Authority retains visibility of when such payments are scheduled to be paid.
- 2.7 After submitting the draft Payment Planner in accordance with Paragraphs 2.3 and 2.4 the Authority will in a timely manner review and raise any queries and then the Supplier will respond and resolve such queries and, in any event, no more than five (5) Working Days from the date of issue of the draft Payment Planner and the Supplier will then issue the final Payment Planner one (1) Working Day thereafter and in any event before the Payment Planner meeting referred to in Paragraph 2.8.

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 2.8 No more than seventeen (17) Working Days from the start of the month the Supplier will then attend a Payment Planner review meeting with the Authority, where the proposed Charges in the Payment Planner will be reviewed, discussed, agreed, or disputed by the Authority. Any disputed or missing Charges which require clarification or where additional information is being sought or cannot be cleared by the time the final Payment Planner is submitted are to be deferred to the next payment month and recorded in the Payment Planner for consideration in the next Payment Planner review meeting. This allows for the un-disputed items to be paid.
- 2.9 Following the Payment Planner review meeting the Supplier is to submit draft invoices for undisputed items, no more than five (5) Working Days after the Payment Planner review meeting. The Authority will use the final Payment Planner and draft invoices to sanction the release of funds. The Supplier will be informed when this occurs to enable them to invoice as described in this Schedule 15.
- 2.10 The Authority will review and raise any queries in a timely manner on the draft invoices and then the Supplier will respond and resolve such queries and issue the final invoices within two (2) Working Days of submission of the draft invoices in accordance with Paragraph 2.9. The thirty (30) calendar days payment terms set out in Paragraph 3.1 of this Part E will commence from receipt of final undisputed and valid invoices.
- 2.11 Invoices should only be submitted to the Authority once the Authority has agreed the final Payment Planner. The invoiced amounts should exactly match the values and purchase order numbers contained in the Payment Planner to facilitate their prompt payment. Delays in the timely submission of the Payment Planner or invoicing errors will result in delayed payments by the Authority, and in the event of invoicing errors will require correct invoices to be reissued by the Supplier before payment shall be made.
- 2.12 A diagram summarising the key steps, timescales and documents required in the Payment Planner process described in this Paragraph 2 is set out in Annex G (*Payment Planner*) below. The diagram is for illustration purposes only.

3 PAYMENT TERMS

- 3.1 Subject to the relevant provisions of this Schedule, the Authority shall make payment to the Supplier within thirty (30) days of verifying that the invoice is valid and undisputed.
- 3.2 Unless the Parties agree otherwise in writing, all Supplier invoices shall be paid in sterling by electronic transfer of funds to the bank account that the Supplier has specified on its invoice.

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Annex A: Key Milestones, Payment Milestones, Milestone Payments and Delay Payments

Milestone No.	Milestone Description	Milestone Date	Payment Milestone (Y/N)	Milestone Payment	Milestone Retention (20%)	Linked Milestone(s) (see para 3.3 of Part A, Sch 15)	Release of Milestone Retention ? (see para 3.3 of Part A, Sch 15)	Key Milestone (Delay Payments payable?)	Amount of Delay Payments	Delay Deduction Period (and maximum Delay Payments)
Milestone M6	Low Level Designs complete	Effective Date + 58 Working Days	Yes	[REDACTED]	[REDACTED]	M1a, M1b, M2, M3, M4 and M5	N/A	No	N/A	N/A
Milestone M10	Operational Services Acceptance (ATP Milestone)	Effective Date + 122 Working Days	Yes	[REDACTED]	[REDACTED]	M7, M8 and M9	N/A	Yes	[REDACTED]	[REDACTED]
Milestone M11	Gateway Services Transition (ATP Milestone)	Effective Date + 138 Working Days	Yes	[REDACTED]	[REDACTED]	M10	N/A	Yes	[REDACTED]	[REDACTED]

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone No.	Milestone Description	Milestone Date	Payment Milestone (Y/N)	Milestone Payment	Milestone Retention (20%)	Linked Milestone(s) (see para 3.3 of Part A, Sch 15)	Release of Milestone Retention ? (see para 3.3 of Part A, Sch 15)	Key Milestone (Delay Payments payable?)	Amount of Delay Payments	Delay Deduction Period (and maximum Delay Payments)
Milestone M12	Pilot Site Transitions (ATP Milestone)	Effective Date + 159 Working Days	Yes	[REDACTED]	[REDACTED]	M10	N/A	Yes	[REDACTED]	[REDACTED]
Milestone M13	Site Transitions – Phase 1	Effective Date + 236 Working Days	Yes	[REDACTED]	[REDACTED]	M10 and M12	20% of current value of Milestone Retention Fund released	Yes	[REDACTED]	[REDACTED]
Milestone M14	Site Transitions – Phase 2	Effective Date + 318 Working Days	Yes	[REDACTED]	[REDACTED]	M10 and M12	20% of value of Milestone Retention Fund released	Yes	[REDACTED]	[REDACTED]
Milestone M15	Site Transitions – Phase 3	Effective Date + 400 Working Days	Yes	[REDACTED]	[REDACTED]	M10 and M12	20% of value of Milestone Retention Fund released	Yes	[REDACTED]	[REDACTED]

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Milestone No.	Milestone Description	Milestone Date	Payment Milestone (Y/N)	Milestone Payment	Milestone Retention (20%)	Linked Milestone(s) (see para 3.3 of Part A, Sch 15)	Release of Milestone Retention ? (see para 3.3 of Part A, Sch 15)	Key Milestone (Delay Payments payable?)	Amount of Delay Payments	Delay Deduction Period (and maximum Delay Payments)
Milestone M16	Site Transitions – Phase 4 (CPP Milestone)	Effective Date + 482 Working Days	Yes	[REDACTED]	N/A	M13, M14 and M15	Remainder of Milestone Retention Fund released	Yes	[REDACTED]	[REDACTED]
Milestone M17	Transition Complete	Effective Date + 507 Working Days	No	N/A	N/A	M12, M13, M14, M15 and M16	N/A	Yes	[REDACTED]	[REDACTED]

Table 1: Key Milestones, Payment Milestones, Milestone Payments and Delay Payments

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Annex B: Service Charges**1 Fixed Service Charges**

- 1.1 The Gateway Service Charges shown in Table 2 are subject to Allowable Assumption AA-08 and shall be payable from the date on which Milestone M11 (Gateway Services Transition) is Achieved.
- 1.2 The Gateway Test System Charges shall be payable from the date on which Milestone M10 (Operational Services Acceptance) is Achieved.

Charges	Charge Item	Requirements Reference					
			Month 1	Months 2 - 11	Months 12 - 23	Months 24 - 33	Months 34 to 113
Gateway Service Charges	DC Transit LAN Service Charges	Technical Requirements, Paragraph 4.3.1					
	DC Interconnect Service Charges	Technical Requirements, Paragraph 4.3.1	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
	ViSOR SSL VPN Service Charges	Technical Requirements, Paragraph 4.5.2					
Charges	Charge Item	Requirements Reference					
			Month 1	Months 2 - 11	Months 12 - 23	Months 24 - 33	Months 34 to 113
Gateway Test System Charges	Gateway Test System Charges	Paragraph 5.3.1 of the Technical Requirements	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
For illustration: Forecast Charges per Contract Year (subject to Allowable Assumption AA-08)							

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Charges	Charge Item	Requirements Reference	Contract Year 1	Contract Year 2	Contract Year 3	Contract Year 4	Contract Years 5 - 10
Gateway Service Charges	DC Transit LAN Service Charges	Technical Requirements, Paragraph 4.3.1 of the	[REDACTED]				
	DC Interconnect Service Charges	Technical Requirements, Paragraph 4.3.1 of the		[REDACTED]			
	ViSOR SSL VPN Service Charges	Technical Requirements, Paragraph 4.5.2 of the					
Gateway Test System Charges	Gateway Test System Charges	Technical Requirements, Paragraph 5.3.1 of the	[REDACTED]	[REDACTED]			[REDACTED]

Table 2: Fixed Service Charges

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 1.3 The Service Charges shown in Table 3 shall be payable following implementation of the IPAM Service (Optional Services) in accordance with the Optional Services Implementation Plan, whereby the monthly recurring Charges shall be determined according to the minimum period ("MP") committed under the relevant Change:

Charges	Requirements Reference	Monthly recurring Charge			
		1-year MP	2-year MP	3-year MP	4 or more years' MP
IPAM Service Charges	Technical Requirements, Paragraph 5.6.1	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
		For illustration: 12 months' Charges			
		1-year MP	2-year MP	3-year MP	4 or more years' MP
IPAM Service Charges	Technical Requirements, Paragraph 5.6.1 of the	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Table 3: Fixed Service Charges for Optional Services

2 Volume Based Service Charges

- 2.1 The following Service Charges shall be payable from the relevant Operational Service Commencement Dates for each Authority Site).

Charges	Charge Item	Requirements Reference	Amount
Transport Service Charges	DIA Bearer Service Charges	Technical Requirements, Paragraphs 3.2.1 and 3.2.3	See Paragraphs 2.1.1 and 2.1.2
	Primary Fixed Broadband Service Charges	Technical Requirements, Paragraphs 3.2.1 and 3.2.4	See Paragraph 2.1.3
	Ancillary Fixed Broadband Service Charges		

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

	Mobile Broadband Service Charges	Technical Requirements, Paragraphs 3.2.1 and 3.2.5	

Table 4: Summary Volume Based Service Charges

- 2.1.1 Where the bearer capacity of an Access Circuit is unchanged from the bearer capacity listed for the relevant Authority Site in the Contract Inception Report, and the relevant Authority Site is identified in the Contract Inception Report as having been priced, the Charges shown in Table 5 shall apply:

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

	Site Architecture	Scenario 1 Yr1 to 3 DIA CDR (Mbps per Link)	Access Circuit Capacity (Mbps per Link)	One-time Charges per link ("OTC")		Monthly recurring Charges per link ("MRC")	
				Bearer Installation Charge	Device Installation Charge	Bearer Rental Charge	Managed Service Charge
	Single Link	100	1000				
	Single Link	150	1000				
	Single Link	200	1000				
	Single Link	300	1000				
	Single Link	400	1000				
	Dual Link	100	1000				
	Dual Link	150	1000				
	Dual Link	200	1000				
	Dual Link	300	1000				
	Dual Link	400	1000				
	Dual Link	500	1000				
	Dual Link	600	1000				
	Dual Link	700	1000				
	Dual Link	800	1000				
	Dual Link	1000	1000				
	Dual Link	100	10000				
	Dual Link	150	10000				
	Dual Link	200	10000				
	Dual Link	300	10000				
	Dual Link	400	10000				
	Dual Link	500	10000				
	Dual Link	600	10000				
	Dual Link	1500	10000				
	Dual Link	3000	10000				

Table 5: DIA Bearer Service Charges

Note: Scenario 1 Yr1 to 3 DIA CDR (MBps per Link) in Table 5 is shown solely for the purpose of identifying the relevant Authority Sites within the Contract Inception Report. In accordance with Paragraph 2.7 to Part A of Schedule

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

22 (Change Control Procedure, Service Requests and Projects), the CDR does not affect the Charges where such CDR is within the bearer capacity of the relevant Access Circuit.

2.1.2 Where, pursuant to the Change Control Procedure:

- (a) the bearer capacity of an Access Circuit differs from the bearer capacity listed for the relevant Authority Site in the Contract Inception Report; or
- (b) an Access Circuit is implemented additional to the Access Circuits listed in the Contract Inception Report; or
- (c) an Authority Site is listed in the Contract Inception Report at the Effective Date and is identified as not being priced in the column headed 'Authority Site included in the CIR at the Effective Date and priced [yes/no]',

then the DIA Bearer Service Charges for the relevant Access Circuit shall be the sum of:

- (i) the OTC (as defined in Table 5) for the relevant Access Circuit capacity; and
- (ii) the managed service charge shown in Table 5; and
- (iii) the bearer rental charge for the relevant Access Circuit shown in Table 6 (as updated under the relevant Change).

Authority Site ID	Authority Site	Site Architecture	Access Circuit Capacity (Mbps per Link)	Monthly Bearer Rental Charge (per link)
[insert]	[insert]	[Single] [Dual] Link	[1000] [10000]	£[insert]

Table 6 - DIA Bearer Rental Charges (where different from Table 5)

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

2.1.3 Transport Service Charges for Fixed Broadband and Mobile Broadband shall be as shown in Table 7, per fixed line and per mobile broadband hub Device:

Charge	Requirements reference	Technology	One-time Charge upon installation ("OTC")	Monthly recurring Charges (MRC)	
				Broadband Service Charge	Incident Resolution Service Charge
Primary Fixed Broadband Service Charges	Technical Requirements: Paragraphs 3.2.1 and 3.2.4	Business Grade, ASDL, ASDL2, FTTC, FTTP			
Ancillary Fixed Broadband Service Charges	Technical Requirements: Paragraphs 3.2.1 and 3.2.4				
Mobile Broadband Service Charges	Technical Requirements: Paragraphs 3.2.1 and 3.2.5	4G			
		5G			

Table 7: Primary Fixed Broadband, Ancillary Fixed Broadband and Mobile Broadband Service Charges

2.2 The Service Charges shown in Table 8, Table 9 and Table 10 shall be applicable following the implementation of the relevant Optional Services in accordance with the Optional Services Implementation Plan.

Charges	Requirements Reference	Monthly Charge
Data Centre Internet Service Charges	Paragraph 4.4.1 of the Technical Requirements	See Table 9 and Table 10 below
SASE Services Charges	Paragraph 6 of the Technical Requirements, and Paragraphs 6.8.5.1, 6.8.5.2 and 6.8.5.3 of the Service Management Requirements	

Table 8: Summary Volume Based Charges for Optional Services

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Charge Item	Requirements Reference	Site	DIA CDR (Mbps per Link)	Access Circuit Capacity (Mbps per Link)	One-time Charges per link ("OTC")		Monthly recurring Charges per link ("MRC")	
					Bearer Installation Charge	Device Installation Charge	Bearer Rental Charge	Managed Service Charge
Data Centre Internet Service Charges	Paragraph 4.4.1 of the Technical Requirements	Ark Building A101	10,000	10,000				
		Ark Building A101	10,000	10,000				
		Ark Building P1	10,000	10,000				
		Ark Building P1	10,000	10,000				
		Cable and Wireless Park Royal Data Centre	10,000	10,000				
		Cable and Wireless Park Royal Data Centre	10,000	10,000				
		Cable and Wireless Swindon Data Centre	10,000	10,000				
		Cable and Wireless Swindon Data Centre	10,000	10,000				

Table 9: Detailed Volume Based Service Charges for Data Centre Internet Service Charges (Optional Services)

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Charges	Requirements reference	Basis of Charges
SASE Services Charges: Resale	Technical Requirements, Paragraph 6.2 (resale of [REDACTED] products and services)	[REDACTED]
SASE Services Charges: Professional services	Technical Requirements, Paragraph 6.3 (professional services for SASE and SD-WAN)	Annex C: Rate Card
SASE Services Charges: Field Services	Service Management Requirements: (a) Paragraph 6.8.5.1 (SASE Service Incidents, and relevant Requests) (b) Paragraph 6.8.5.2 (agency management in support of 6.8.5.1)	(a) Annex C: Rate Card (b) No Charges
SASE Services Charges: Distributed spares	Service Management Requirements, Paragraph 6.8.5.3 (distributed spares management)	[REDACTED]

Table 10: Detailed Volume Based Service Charges for Optional Services, SASE Services**3 Catalogue Item Charges**

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Ref.	Description	Unit	Lead time	One-time Charge 1 st instance	One-time Charge subsequent instances	Volume of free of charge Service Requests per month	Maximum instances at the same Site on the same day
WAN-SR-01	Modify Circuit bandwidth (CDR) on a bearer	Per instance	Immediate	[REDACTED]			
WAN-HR-01	Provision of a new 100Mbps Access Circuit (DIA)	Per instance (at the same Site, on the same day)	60 Working Days				
WAN-HR-02	Provision of a new 1Gbps Access Circuit (DIA)	Per instance (at the same Site, on the same day)	60 Working Days				
WAN-HR-03	Provision of a new 10Gbps Access Circuit (DIA)	Per instance (at the same Site, on the same day)	60 Working Days				
WAN-HR-04a	WAN Connectivity Field Services: Device installation (Technical Requirements, Paragraph 2.2.1)	Per instance (at the same Site, on the same day)	15 Working Days				
WAN-HR-04b	WAN Connectivity Field Services: Device decommissioning (Technical Requirements, Paragraphs 2.2.2.1 to 2.2.2.3) without secure destruction	Per instance (at the same Site, on the same day)	15 Working Days				
WAN-HR-05	Access Circuit cease	Per instance (at the same Site, on the same day)	22 Working Days				

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Ref.	Description	Unit	Lead time	One-time Charge 1 st instance	One-time Charge subsequent instances	Volume of free of charge Service Requests per month	Maximum instances at the same Site on the same day
WAN-HR-06	Access Circuit feasibility check: desktop survey of a new Access Circuit location (as a standalone activity separate from installation of Access Circuits)	Per instance (at the same Site, on the same day)	5 Working Days	[REDACTED]			
WAN-HR-07	Provision of a new fixed broadband Access Circuit - Primary Fixed Broadband Services (Paragraph 2.3.4 of the Technical Requirements)	Per instance (at the same Site, on the same day)	15 Working Days				
WAN-HR-08	Provision of a new fixed broadband Access Circuit - Ancillary Fixed Broadband Services (Paragraph 2.3.4 of the Technical Requirements)	Per instance (at the same Site, on the same day)	15 Working Days				
WAN-HR-09	Not used	N/A	N/A				
WAN-HR-10	Decommission and secure disposal of legacy WAN CPE (i.e. CPE used for Transitional Services and/or Preceding Services) in accordance with the Standards	Per instance (at the same Site, on the same day)	10 Working Days				

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Ref.	Description	Unit	Lead time	One-time Charge 1 st instance	One-time Charge subsequent instances	Volume of free of charge Service Requests per month	Maximum instances at the same Site on the same day
WAN-[Ref no. to be assigned] *	Field spare swap of SD-WAN Edge Device, including managing return to vendor (Service Management Requirements, Paragraph 6.8.5 – SASE Services Optional Service)	Per instance (at the same Site, on the same day)	4 Service Hours	[REDACTED]			

Table 11: Catalogue Item Charges

*Note that this line will not be added to the Product & Services Catalogue unless the relevant Optional Service is implemented.

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Annex C: Rate Card

Code	Role/Job Title	Daily Rate (£) 1 - 60 Days	Daily Rate (£) 61 - 120 Days	Daily Rate (£) 121 - 200 Days	Daily Rate (£) 201 - 300 Days	Daily Rate (£) 300+ Days
TA1	Senior Architect					
TA2	Architect					
TE1	Senior Network Engineer					
TE2	Network Engineer 1					
TE3	Senior Field Engineer					
TE4	Field Engineer: Level 1					
TE5	Field Engineer: Level 2					
TS1	1st Line Technical Support					
TS2	2nd Line Technical Support					
TS3	3rd Line Technical Support					
TS4	4th Line Technical Support					
SA1	Security Architect					
SA2	Senior Security Administration					
SA3	Security Administration					
TST1	Testing Manager					
TST2	Senior Tester					
TST3	Tester					
BA1	Senior Business Analyst					
BA2	Business Analyst					
PM1	Programme Manager					
PM2	Senior Project Manager					
PM3	Project Manager					
PM4	Project Task Manager					
PM5	Project PMO					

Table 12: Rate Card

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Annex D: Pro-Forma Certificate of Costs

I **[name of CFO or Director of Finance or equivalent as agreed in advance in writing with the Authority]** of **[insert name of Supplier]**, certify that the financial information provided as part of this Certificate of Costs, incurred in relation to the **[insert name/reference for the Contract]** (the “Contract”) in relation to the following **[Milestone/Milestone Group]**:

[Insert details of Milestone/Milestone Group]

- 1 has been reasonably and properly incurred in accordance with **[name of Supplier]**'s books, accounts, other documents and records;
- 2 is accurate and not misleading in all key respects; and
- 3 is in conformity with the Contract and with all generally accepted accounting principles within the United Kingdom.

Signed **[Director of Finance or equivalent]**

[Name of Supplier]

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Annex E: Risk Register

No risks and contingencies have been identified as at the Effective Date.

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6	Column 7	Column 8	Column 9	Column 10	Column 11	Column 12
Risk Number	Risk Name	Description of risk	Timing	Likelihood	Impact (£)	Impact (description)	Mitigation (description)	Cost of mitigation	Post-mitigation impact (£)	Forecast Contingency Costs	Owner

Table 13: Risk Register

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Annex F: Allowable Assumptions

Ref	Description of proposed Allowable Assumption	Impact on the Implementation Plan if the Allowable Assumption is not accurate	Cost Impact (maximum, minimum and most likely values if the Allowable Assumption is not accurate)	Basis of Calculation of Cost Impact	Applicable Profit Margin	Charge Impact (maximum, minimum and most likely values if the Allowable Assumption is not accurate)	Verification Method (how the Supplier will verify the Allowable Assumption)	Trigger for Invocation (what will determine that the Implementation Plan and/or Financial Model may require adjustment for the Allowable Assumption)	Period of Impact (period that the updated assumption will have an impact)	Expiry Date (Date at which the Allowable Assumption expires)	Assumptions Value £
AA-01	It is assumed that, in the event the Authority requires an Optional Service in accordance with Clause 5.10, there will be no Transferring Authority Employees or Transferring Former Supplier Employees.	None. Any impact on the implementation of the relevant Optional Service will be identified by Impact Assessment under the Change Control Procedure.	To be identified by Impact Assessment under the Change Control Procedure	In accordance with the Change Control Procedure	None	To be identified by Impact Assessment under the Change Control Procedure	Due diligence at time of Impact Assessment	Execution of relevant Change Authorisation Note	As described in the relevant Change Authorisation Note	Date of execution of first Change Authorisation Note, per Optional Service	No estimate possible

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Ref	Description of proposed Allowable Assumption	Impact on the Implementation Plan if the Allowable Assumption is not accurate	Cost Impact (maximum, minimum and most likely values if the Allowable Assumption is not accurate)	Basis of Calculation of Cost Impact	Applicable Profit Margin	Charge Impact (maximum, minimum and most likely values if the Allowable Assumption is not accurate)	Verification Method (how the Supplier will verify the Allowable Assumption)	Trigger for Invocation (what will determine that the Implementation Plan and/or Financial Model may require adjustment for the Allowable Assumption)	Period of Impact (period that the updated assumption will have an impact)	Expiry Date (Date at which the Allowable Assumption expires)	Assumptions Value £
AA-02	It is assumed that – immediately prior to the Operational Service Commencement Date for Gateway Services – the Gateway System and the Transitional Services equivalent to the following Services meet all the relevant Authority Requirements: (a) Gateway LAN services (b) Peering Services (c) Gateway Test System and it is assumed that no remedial works will be required under the Transitional Services solely in order for the above standard to be met.	Only if the Authority requires remedial works in order for Milestone 11 (Gateway Services transition) to be Achieved: potential delay to Milestone 11	To be identified in relevant Project Work Order(s) (if any) at Milestone 10 (WAN Services Acceptance)	In accordance with the Change Control Procedure	In accordance with Financial Model	To be identified in relevant Project Work Order(s) (if any) at Milestone 10 (WAN Services Acceptance)	Due diligence following mobilisation of Transitional Services (Milestone 1b), to prepare Risk Register updates for Milestone 10 (WAN Services Acceptance)	Approval of updated Risk Register containing relevant activities following review in accordance with paragraph 7.1 of Part C of this Schedule 15	As described in the Risk Register (as updated)	Date of Approval of updated Risk Register containing relevant activities	No estimate possible

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Ref	Description of proposed Allowable Assumption	Impact on the Implementation Plan if the Allowable Assumption is not accurate	Cost Impact (maximum, minimum and most likely values if the Allowable Assumption is not accurate)	Basis of Calculation of Cost Impact	Applicable Profit Margin	Charge Impact (maximum, minimum and most likely values if the Allowable Assumption is not accurate)	Verification Method (how the Supplier will verify the Allowable Assumption)	Trigger for Invocation (what will determine that the Implementation Plan and/or Financial Model may require adjustment for the Allowable Assumption)	Period of Impact (period that the updated assumption will have an impact)	Expiry Date (Date at which the Allowable Assumption expires)	Assumptions Value £
AA-03	It is assumed that [REDACTED] End Users will require access to the Supplier's monitoring and reporting functionality.	None	Assumes cost is included in the WAN Service Management Charges.	Assumes cost is included in the WAN Service Management Charges.	N/A	[REDACTED]	Supplier to request confirmed End User volume from Authority	Confirmed End User volume provided by Authority	The Term, unless otherwise agreed	Milestone Achievement Date for Milestone 5 (Service and Solution Design complete)	[REDACTED]
AA-04	Not used	-	-	-	-	-	-	-	-	-	-

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Ref	Description of proposed Allowable Assumption	Impact on the Implementation Plan if the Allowable Assumption is not accurate	Cost Impact (maximum, minimum and most likely values if the Allowable Assumption is not accurate)	Basis of Calculation of Cost Impact	Applicable Profit Margin	Charge Impact (maximum, minimum and most likely values if the Allowable Assumption is not accurate)	Verification Method (how the Supplier will verify the Allowable Assumption)	Trigger for Invocation (what will determine that the Implementation Plan and/or Financial Model may require adjustment for the Allowable Assumption)	Period of Impact (period that the updated assumption will have an impact)	Expiry Date (Date at which the Allowable Assumption expires)	Assumptions Value £
AA-05	It is assumed that the Performance Indicator "Proposal Turnaround" will be measured and monitored by the Authority and/or Authority System.	None	[REDACTED]	1 Day PS per month in Operational Delivery	20%	[REDACTED]	Due diligence with the Authority during development of the relevant Service Design Packages	Approval of the relevant Service Design Packages	From the relevant Operational Service Commencement Dates through the remainder of the Term	Milestone Date for Milestone M10 (WAN Service acceptance)	[REDACTED]

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Ref	Description of proposed Allowable Assumption	Impact on the Implementation Plan if the Allowable Assumption is not accurate	Cost Impact (maximum, minimum and most likely values if the Allowable Assumption is not accurate)	Basis of Calculation of Cost Impact	Applicable Profit Margin	Charge Impact (maximum, minimum and most likely values if the Allowable Assumption is not accurate)	Verification Method (how the Supplier will verify the Allowable Assumption)	Trigger for Invocation (what will determine that the Implementation Plan and/or Financial Model may require adjustment for the Allowable Assumption)	Period of Impact (period that the updated assumption will have an impact)	Expiry Date (Date at which the Allowable Assumption expires)	Assumptions Value £
AA-06	It is assumed that the Performance Indicators "Security Incident Response Time" and "Security Incident Resolution Time" will be measured and monitored by the Authority and/or Authority System.	None	[REDACTED]	1 Day PS per month in Operational Delivery	20%	[REDACTED]	Due diligence with the Authority during development of the relevant Service Design Packages	Approval of the relevant Service Design Packages	From the relevant Operational Service Commencement Dates through the remainder of the Term	Milestone Date for Milestone M10 (WAN Service acceptance)	[REDACTED]

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Ref	Description of proposed Allowable Assumption	Impact on the Implementation Plan if the Allowable Assumption is not accurate	Cost Impact (maximum, minimum and most likely values if the Allowable Assumption is not accurate)	Basis of Calculation of Cost Impact	Applicable Profit Margin	Charge Impact (maximum, minimum and most likely values if the Allowable Assumption is not accurate)	Verification Method (how the Supplier will verify the Allowable Assumption)	Trigger for Invocation (what will determine that the Implementation Plan and/or Financial Model may require adjustment for the Allowable Assumption)	Period of Impact (period that the updated assumption will have an impact)	Expiry Date (Date at which the Allowable Assumption expires)	Assumptions Value £
AA-07	Not used	-	-	-	-	-	-	-	-	-	-
AA-08	It is assumed that where Devices of the Gateway System are indicated within the FRT as to be decommissioned, the relevant Devices will be decommissioned on the date shown.	None	To be identified by Impact Assessment under the Change Control Procedure	Actual impact	10.4%	In accordance with the Change Control Procedure	Review of work in progress project(s) for rationalisation of Gateway System	Device decommissioning schedule updated and agreed with the Authority	From the relevant Operational Service Commencement Date until the relevant Devices are decommissioned	Milestone Date for Milestone M6 (Low Level Designs complete)	No estimate possible

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Ref	Description of proposed Allowable Assumption	Impact on the Implementation Plan if the Allowable Assumption is not accurate	Cost Impact (maximum, minimum and most likely values if the Allowable Assumption is not accurate)	Basis of Calculation of Cost Impact	Applicable Profit Margin	Charge Impact (maximum, minimum and most likely values if the Allowable Assumption is not accurate)	Verification Method (how the Supplier will verify the Allowable Assumption)	Trigger for Invocation (what will determine that the Implementation Plan and/or Financial Model may require adjustment for the Allowable Assumption)	Period of Impact (period that the updated assumption will have an impact)	Expiry Date (Date at which the Allowable Assumption expires)	Assumptions Value £
AA-09	"Capacity Management" Performance Indicator It is assumed that any replacement measure of Capacity Management required under Transition Requirements, Paragraph 7.2.1.22, shall not require additional allocation of Supplier Personnel or additional Supplier Equipment or Licensed Software compared to measurement as <i>"the percentage of Resolved Service Incidents in a Service Period without a capacity-related Resolution code as recorded in the ITSM Toolset"</i> .	Any impact on the implementation will be identified by Impact Assessment under the Change Control Procedure.	To be identified during the review of the Performance Indicator for Capacity Management in Milestone 5 (Service and Solution Design complete)	In accordance with the Change Control Procedure	10.4%	In accordance with the Change Control Procedure	Review of notice given by the Authority under Paragraph 7.2.1.22 of the Transition Requirements	Expiry of notice period for relevant notice given by the Authority under Paragraph 7.2.1.22 of the Transition Requirements	From the relevant Operational Service Commencement Dates through the remainder of the Term	Milestone Date for Milestone M5 (Service and Solution Design complete)	No estimate possible

Table 14: Allowable Assumptions

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Annex G: Payment Planner

The Supplier shall provide to the Authority the Financial Reports in the same software package (Microsoft Excel or Microsoft Word), layout and format as the blank templates which have been issued by the Authority to the Supplier on or before the Effective Date for the purposes of this Contract. The Authority shall be entitled to modify the template for any Financial Report by giving written notice to the Supplier, including a copy of the updated template.

Payment Planner Cycle

NOTE: The diagram below has been included for illustration purposes only to summarise and illustrate the Payment Planner process as set out in Paragraph 2 (*Payment Planner*) of Part E (*Invoicing and Payment Terms*) of this Schedule 15. In the event of any conflict or discrepancy between the diagram and Paragraph 2 (*Payment Planner*) of Part E (*Invoicing and Payment Terms*) of this Schedule 15, Paragraph 2 (*Payment Planner*) shall take precedence.

SCHEDULE 15 (CHARGES AND INVOICING)

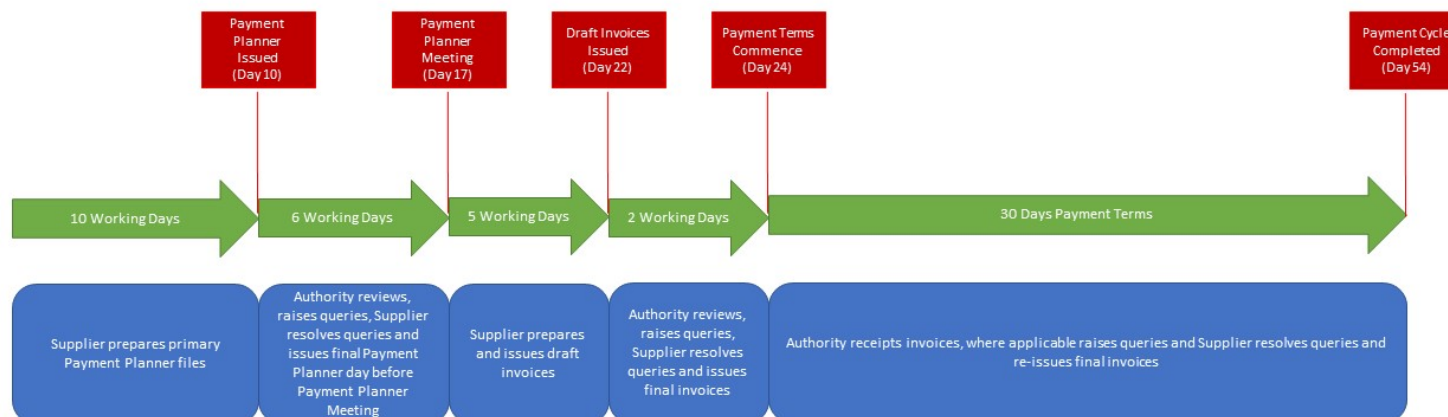
Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Payment Cycle



General Principles

Single Payment Planner to be issued at the start of the Payment Cycle

Payment Planner to only be amended ahead of Payment Planner meeting with Authority raised queries

Payment Planner meeting is to approve charges and not to be used to discuss issues/queries

Any missed items to be raised the following monthly cycle (noted on the planner as a future charge)

Payment Planner and Invoicing must always agree

SCHEDULE 15 (CHARGES AND INVOICING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Annex H: Illustration of Service Points Accrual and Service Credits

See:

Evolve - WAN Contract - Schedule 15 (Charges and Invoicing) Annex H



Ministry
of Justice

Annex H: Illustration of Service Points Accrual and Service Credits

Version Control Table

Issue No	Issue Date:	Issue Author:	Version Narrative
0.1	1/24/2025	MoJ	Issued for for use with Preferred Bidder

This Annex H sets out, for information only, example Service Credits calculations for the nine KPIs to illustrate how the provisions of Paragraph 3 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing) will be applied:

- KPI-01a Availability: WAN Connectivity
- KPI-01b Availability: Gateway Services
- KPI-02 Incident Resolution Times: Severity 1 Service Incidents and Severity 2 Service Incidents
- KPI-03 Incident Resolution Times: Severity 3 Service Incidents
- KPI-04 Security Incident Response Time
- KPI-05 Security Incident Resolution Time
- KPI-06 Change Management
- KPI-07 Service Request Fulfilment
- KPI-08 Knowledge Management

In this Annex H, the definitions as stated in Schedule 1 (Definitions), Schedule 3 (Performance Levels) and Schedule 15 (Charges and Invoicing) shall apply.

Availability: WAN Connectivity KPI (KPI-01a) - Service Credit Illustration

This worksheet provides, for information only, a Service Credit calculation example for the Availability: WAN Connectivity KPI (KPI-01a) to illustrate how the provisions of Paragraph 3 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing) will be applied.

Transport Service Charges

For the purpose of this example, the Transport Service Charges for an Authority Site of each Site Type is assumed as follows:

Site Type	Monthly Transport Service Charges
Gold Site	[REDACTED]
Silver Site	[REDACTED]
Bronze Site	[REDACTED]

Transport Service Charges are the Service Charges for the provision of the Transport Services as set out in Paragraph 2.1 of Annex B (Service Charges) of Schedule 15 (Charges and Invoicing).

Service Credit Increments

The Service Credit Increments for KPI-01a for each Authority Site are calculated in accordance with Paragraph 3.8 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing).

Site Type	Target Performance Level	KPI Service Threshold	Number of Service Credit Increments
	<i>A</i>	<i>B</i>	<i>D</i> <i>(A-B)/0.01%</i>
Gold Site	99.99%	98.99%	100
Silver Site	99.95%	97.99%	196
Bronze Site	99.90%	97.99%	191

Service Credit Point Value

The Service Credit Point Values for KPI-01a for each Authority Site are calculated in accordance with Paragraph 3.7 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing).

Site Type	Transport Service Charges Assumption (£)	At Risk Percentage (%)	At Risk Amount (£)	Service Credit Point Value (£)
	<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i> <i>/(100 or 196 or 191)</i>
Gold Site	[REDACTED]	80.00%	[REDACTED]	[REDACTED]
Silver Site	[REDACTED]	65.00%	[REDACTED]	[REDACTED]
Bronze Site	[REDACTED]	50.00%	[REDACTED]	[REDACTED]

Service Credit Calculation

For KPI-01b, one Service Credit Point will accrue for each 0.01% below the Target Performance Level in accordance with Table 2 of Paragraph 1.1 of Part A of Annex 1 of Schedule 3 (Performance Levels).

The Service Credit due in respect of KPI-01a for each Authority Site is calculated in accordance with Paragraph 3.6 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing).

The table below illustrates how different Availability performance across Authority Sites will result in differing numbers of Service Points and thus values of Service Credits due in that Service Period.

For example, if during a particular Service Period, three Authority Sites fail to achieve the relevant Availability Target Performance Level:

- a Gold Site achieving an Availability of **99.70%**;
- a Silver Site achieving an Availability of **99.00%**; and
- a Bronze Site achieving an Availability of **98.00%** (see rows 40, 46 and 52 in the table below).

In this example, the Service Credits due will be: [REDACTED]

Levels	Site Type	Target Performance Level	Achieved Availability	Service Points Accrued	Service Credit Due (£)
		A	B	C (A - B)/0.01%	
Target Performance Level	Gold Site	99.99%	99.99%	0	
Minor KPI Failure	Gold Site	99.99%	99.70%	29	
Serious KPI Failure	Silver Site	99.95%	99.50%	45	
Severe KPI Failure	Gold Site	99.99%	99.00%	99	
KPI Service Threshold	Gold Site	99.99%	98.99%	100	
Target Performance Level	Silver Site	99.95%	99.95%	0	
Minor KPI Failure	Silver Site	99.95%	99.50%	45	
Serious KPI Failure	Silver Site	99.95%	99.00%	95	
Severe KPI Failure	Silver Site	99.95%	98.00%	195	
KPI Service Threshold	Silver Site	99.95%	97.99%	196	
Target Performance Level	Bronze Site	99.90%	99.90%	0	
Minor KPI Failure	Bronze Site	99.90%	99.50%	40	
Serious KPI Failure	Bronze Site	99.90%	99.00%	90	
Severe KPI Failure	Bronze Site	99.90%	98.00%	190	
KPI Service Threshold	Bronze Site	99.90%	97.99%	191	

If during the subsequent Service Period, the **same** three Authority Sites fail to achieve the Availability Target Performance Level achieving the same Availability as the previous Service Period (and all other things being equal), then three Repeat KPI Failures would have occurred. The Service Credits due (in accordance with Paragraph 3 of Part A of Schedule 3 (Performance Levels)) will be twice that of the previous Service Period, and would be a total of: [REDACTED]

Availability: Gateway Services KPI (KPI-01b) - Service Credit Illustration

This worksheet provides, for information only, a Service Credit calculation example for the Availability: Gateway Services KPI (KPI-01b) to illustrate how the provisions of Paragraph 3 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing) will be applied.

Assumption - Gateway Service Charges

For the purpose of this example, the Gateway Service Charges are assumed as follows:

Item	Monthly charge
Gateway Service Charges	[REDACTED]

Service Credit Calculation

For KPI-01b, one Service Point will accrue for each 0.01% below the Target Performance Level for a failure of any of the Gateway Services to achieve the relevant Target Performance Level in accordance with Table 2 of Paragraph 1.1 of Part A of Annex 1 of Schedule 3 (Performance Levels)

The Service Credit due in respect of KPI-01b is calculated in accordance with Paragraph 3.5 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing).

The table below illustrates how different Availability performance will result in differing numbers of Service Points and thus values of Service Credits due in the Service Period. For example, if Availability of the DC Transit LAN in a Service Period is **99.70%**, Service Credits due would be:

[REDACTED]

Performance Levels	Achieved Availability	Target Performance Level	Service Points Accrued	Applicable % Deduction	Gateway Services Service Charges (£)	Service Credit Due (£)
	<i>A</i>	<i>B</i>	<i>C</i> <i>(B-A)/0.01%</i>	<i>D</i>	<i>E</i>	<i>F</i> <i>C x D x E</i>
Target Performance Level	99.99%	99.99%	0	0.01%		
Minor KPI Failure	99.70%	99.99%	29	0.01%		
Serious KPI Failure	99.50%	99.99%	49	0.01%		
Severe KPI Failure	99.00%	99.99%	99	0.01%		
KPI Service Threshold	98.99%	99.99%	100	0.01%		

If during the subsequent Service Period, any one of the Gateway Services fail to achieve the Target Performance Level achieving the same Availability (**99.70%**) as the previous Service Period (and all other things being equal), then a Repeat KPI Failure would have occurred. The Service Credits due (in accordance with Paragraph 3.1 of Part A of Schedule 3 (Performance Levels)) will be twice that of the previous Service Period, and would be a total of: [REDACTED]

Incident Resolution Times: Severity 1 and Severity 2 Service Incidents KPI (KPI-02) - Service Credit Illustration

This worksheet provides, for information only, a Service Credit calculation example for the Incident Resolution Times: Severity 1 and Severity 2 Service Incidents KPI (KPI-02) to illustrate how the provisions of Paragraph 3 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing) will be applied.

Assumptions

For the purpose of this example, the following assumptions have been made:

Item	Monthly Charges
Fixed Service Charges	[REDACTED]
Volume Based Charges	
Fixed Service Charges and Volume Based Charges	

Service Point Accrual

The Service Points accrued in respect of KPI-02 are calculated in accordance with Paragraphs 3.12 and 3.13 of Part B of Annex 1 to Schedule 3 (Performance Levels).

Performance Indicators	Severity 1 Service Incidents	Severity 2 Service Incidents	Service Points - Severity 1 Service Incidents	Service Points - Severity 2 Service Incidents
Target Performance Level	0 minutes late	0 minutes late	0	0
Minor KPI Failure	>1 minute late, up to 2 hours late	>1 minute late, up to 2 hours late	22, then 1 additional per 5 minutes	20, then 1 additional per 6 minutes
Serious KPI Failure	>2 hours late, up to 4 hours late	>2 hours late; up to 8 hours late	46, then 1 additional per 4 minutes	40, then 1 additional per 10 minutes
Severe KPI Failure	>4 hours late, up to 10 hours late	>8 hours late, up to 20 hours late	76, then 1 additional per 2 minutes	76, then 1 additional per 5 minutes
KPI Service Threshold	>10 hours late	>20 hours late	256, then 1 additional per 2 minutes	256, then 1 additional per 5 minutes

Service Credit Calculation

The Service Credit due in respect of KPI-02 is calculated in accordance with Paragraph 3.10 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing).

Severity 1 Service Incidents

The table below illustrates how different delays in the Resolution of Severity 1 Service Incidents will result in differing numbers of Service Points and thus values of Service Credits due in that Service Period. For example, if a Severity 1 Service Incident is resolved 101 minutes late, this would be a Minor KPI Failure, 42 Service Points would accrue and the Service Credits due would be:

[REDACTED]

Performance Indicators	Number of minutes late in resolving the Service Incident	Service Points	Applicable percentage deduction	Fixed Service Charges and Volume Based Charges (£)	Service Credit Due (£)
		A	B	C	D A x B x C
Target Performance Level	0.5	0	0.01%	[REDACTED]	
Minor KPI Failure	101	42	0.01%		
Serious KPI Failure	200	66	0.01%		
Severe KPI Failure	300	106	0.01%		
KPI Service Threshold	700	306	0.01%		

Severity 2 Service Incidents

The table below illustrates how different delays in the Resolution of Severity 2 Service Incidents will result in differing numbers of Service Points and thus values of Service Credits due in that Service Period. For example, if a Severity 2 Service Incident is resolved 400 minutes late, this would be a Serious KPI Failure, 68 Service Points would accrue and the Service Credits due would be:

[REDACTED]

Performance Indicators	Number of minutes late in resolving the Service Incident	Service Points	Applicable percentage deduction	Fixed Service Charges and Volume Based Charges (£)	Service Credit Due (£)
		<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i> <i>A x B x C</i>
Target Performance Level	0.5	0	0.01%	[REDACTED]	
Minor KPI Failure	115	39	0.01%		
Serious KPI Failure	400	68	0.01%		
Severe KPI Failure	600	100	0.01%		
KPI Service Threshold	1400	296	0.01%		

Incident Resolution Times: Severity 3 Service Incidents KPI (KPI-03) - Service Credit Illustration

This worksheet provides, for information only, a Service Credit calculation example for the Incident Resolution Times: Severity 3 Service Incidents KPI (KPI-03) to illustrate how the provisions of Paragraph 3 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing) will be applied.

Assumptions

For the purpose of this example, the following assumptions have been made:

Item	Monthly Charges
Fixed Service Charges	[REDACTED]
Volume Based Charges	
Fixed Service Charges and Volume Based Charges (£)	

Service Point Accrual

The Service Points accrued in respect of KPI-03 are calculated in accordance with Paragraphs 3.12 and 3.13 of Part B of Annex 1 to Schedule 3 (Performance Levels).

Performance Indicators	<100 Severity 3 Service Incidents	>99 Severity 3 Service Incidents	Service Points
Target Performance Level	Up to one Late Severity 3 Service Incident	98%	0
Minor KPI Failure	Two Late Severity 3 Service Incidents	97.51% – 97.99%	10
Serious KPI Failure	Three Late Severity 3 Service Incidents	97.01% – 97.5%	20
Severe KPI Failure	Four Late Severity 3 Service Incidents	96.01% – 97%	30
KPI Service Threshold	Five or more Late Severity 3 Service Incidents	Below 96.01%	40

Service Credit Calculation

The Service Credit due in respect of KPI-03 is calculated in accordance with Paragraph 3.10 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing).

Where there are fewer than 100 Severity 3 Service Incidents in a Service Period

The table below illustrates how different numbers of Late Severity 3 Service Incidents will result in differing numbers of Service Points and thus values of Service Credits due in that Service Period. For example, if there are fewer than 100 Severity 3 Service Incidents in a Service Period and 2 Late Severity 3 Services Incidents, then this would be a Minor KPI Failure, 10 Service Points would accrue and the Service Credits due would be:

[REDACTED]

Performance Indicators	Number of Late Severity 3 Service Incidents	Service Points	Applicable percentage deduction	Fixed Service Charges and Volume Based Charges (£)	Service Credit Due (£)
		<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i> $A \times B \times C$
Target Performance Level	1	0	0.01%	[REDACTED]	
Minor KPI Failure	2	10	0.01%		
Serious KPI Failure	3	20	0.01%		
Severe KPI Failure	4	30	0.01%		
KPI Service Threshold	5	40	0.01%		

Where there are 100 or more Severity 3 Service Incidents in a Service Period

The table below illustrates how different Incident Resolution Time % will result in differing numbers of Service Points and thus values of Service Credits due in that Service Period. For example, if there are 100 or more Severity 3 Service Incidents in a Service Period with a Incident Resolution Time % of 97.7%, then this would be a Minor KPI Failure, 10 Service Points would accrue and the Service Credits due would be:

[REDACTED]

Performance Indicators	Incident Resolution Time %	Service Points	Applicable percentage deduction	Fixed Service Charges and Volume Based Charges (£)	Service Credit Due (£)
		<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i> $A \times B \times C$
Target Performance Level	98.50%	0	0.01%		
Minor KPI Failure	97.70%	10	0.01%		
Serious KPI Failure	97.30%	20	0.01%		
Severe KPI Failure	96.50%	30	0.01%		
KPI Service Threshold	95.00%	40	0.01%		

Security Incident Response Time KPI (KPI-04) - Service Credit Illustration

This worksheet provides, for information only, a Service Credit calculation example for the Security Incident Response Time KPI (KPI-04) to illustrate how the provisions of Paragraph 3 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing) will be applied.

Assumptions

For the purpose of this example, the following assumptions have been made:

Item	Monthly Charges
Fixed Service Charges	[REDACTED]
Volume Based Charges	
Fixed Service Charges and Volume Based Charges (£)	

Service Point Accrual

The Service Points accrued in respect of KPI-04 are calculated in accordance with Paragraphs 4.6 and 4.7 of Part B of Annex 1 to Schedule 3 (Performance Levels).

Performance Indicators	Severity 1 Security Incidents	Service Points - Severity 1 Security Incidents	Severity 2 Security Incidents	Service Points - Severity 2 Security Incidents
Target Performance Level	0 minutes late	0	0 minutes late	0
Minor KPI Failure	>1 minute late, up to 30 minutes late	40, then 4 per minute	>1 minute late, up to 1 hour late	30, then 1 per minute
Serious KPI Failure	>30 minute late, up to 2 hours late	160, then 4 per minute	>1 hour late, up to 4 hours late	90, then 1 per minute
Severe KPI Failure	>2 hours late, up to 3.5 hours late	520, then 4 per minute	>4 hours late, up to 7 hours late	310, then 2 per minute
KPI Service Threshold	>3.5 hours late	880, then 4 per minute	>7 hours late	630, then 2 per minute

Performance Indicators	Severity 3 Security Incidents	Service Points - Severity 3 Service Incidents	Severity 4 Security Incidents	Service Points - Severity 4 Security Incidents
Target Performance Level	0 minutes late	0	≤1 Service Hour late	0
Minor KPI Failure	>1 minute late, up to 4 Service Hours late	20, then 1 per 6 minutes	>1 Service Hour late	0
Serious KPI Failure	>4 Service Hours late, up to 8 Service Hours late	60, then 1 per 6 minutes	N/A	0
Severe KPI Failure	>8 Service Hours late	100, then 1 per 6 minutes	N/A	0
KPI Service Threshold	N/A	N/A	N/A	0

Service Credit Calculation

The Service Credit due in respect of KPI-04 is calculated in accordance with Paragraph 3.10 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing).

Severity 1 Security Incidents

The table below illustrates how different Security Incident Response Times for Severity 1 Security Incidents will result in differing numbers of Service Points and thus values of Service Credits due in that Service Period. For example, if a Severity 1 Security Incident is responded to 20 minutes late, this would be a Minor KPI Failure, 116 Service Points would accrue and the Service Credits due would be:

[REDACTED]

Performance Indicators	Number of minutes late in responding to the Security Incident	Service Points	Applicable percentage deduction	Fixed Service Charges and Volume Based Charges (£)	Service Credit Due (£)
		A	B	C	$\frac{D}{A \times B \times C}$
Target Performance Level	0.5	0	0.01%	[REDACTED]	
Minor KPI Failure	20	116	0.01%		
Serious KPI Failure	60	280	0.01%		
Severe KPI Failure	180	600	0.01%		
KPI Service Threshold	240	1000	0.01%		

Severity 2 Security Incidents

The table below illustrates how different Security Incident Response Times for Severity 2 Security Incidents will result in differing numbers of Service Points and thus values of Service Credits due in that Service Period. For example, if a Severity 2 Security Incident is responded to 150 minutes late, this would be a Serious KPI Failure, 180 Service Points would accrue and the Service Credits due would be:

[REDACTED]

Performance Indicators	Number of minutes late in responding to the Security Incident	Service Points	Applicable percentage deduction	Fixed Service Charges and Volume Based Charges (£)	Service Credit Due (£)
		<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i> $A \times B \times C$
Target Performance Level	0.5	0	0.01%		
Minor KPI Failure	30	59	0.01%		
Serious KPI Failure	150	180	0.01%		
Severe KPI Failure	330	490	0.01%		
KPI Service Threshold	480	750	0.01%		

Severity 3 Security Incidents

The table below illustrates how different Security Incident Response Times for Severity 3 Security Incidents will result in differing numbers of Service Points and thus values of Service Credits due in that Service Period. For example, if a Severity 3 Security Incident is responded to 1 Service Hour (60 minutes) late, this would be a Minor KPI Failure, 30 Service Points would accrue and the Service Credits due would be:

[REDACTED]

Performance Indicators	No. of Service Hours late in responding to the Security Incident	Service Points	Applicable percentage deduction	Fixed Service Charges and Volume Based Charges (£)	Service Credit Due (£)
		<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i> $A \times B \times C$
Target Performance Level	0	0	0.01%		
Minor KPI Failure	1	30	0.01%		
Serious KPI Failure	8	100	0.01%		
Severe KPI Failure	20	220	0.01%		

Security Incident Resolution Time KPI (KPI-05) - Service Credit Illustration (incomplete)

This worksheet provides a Service Credit calculation example for the Security Incident Resolution Time KPI (KPI-05) to illustrate how the provisions of Paragraph 3 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing) will be applied.

Assumptions

For the purpose of this example, the following assumptions have been made:

Item	Monthly Charges
Fixed Service Charges	
Volume Based Charges	
Fixed Service Charges and Volume Based Charges (£)	

Service Point Accrual

The Service Points accrued in respect of KPI-05 are calculated in accordance with Paragraphs 4.9 and 4.10 of Part B of Annex 1 to Schedule 3 (Performance Levels).

Performance Indicators	Severity 1 Security Incidents	Service Points - Severity 1 Security Incidents	Severity 2 Security Incidents	Service Points - Severity 2 Security Incidents	Severity 3 Security Incidents	Service Points - Severity 3 Service Incidents
Target Performance Level	0 minutes late	0	0 minutes late	0	8 hours late	0
Minor KPI Failure	>1 minute late, up to 2 hours late	20, then 1 per 5 minutes	>1 minute late, up to 4 hours late	10, then 1 per 6 minutes	>8 hours late, up to 2 Working Days late	10, then 5 per Service Hour
Serious KPI Failure	>2 hours late, up to 6 hours late	44, then 1 per 4 minutes	>4 hours late, up to 12 hours late	50, then 1 per 6 minutes	>=2 Working Days late, up to 3 Working Days late	50, then 10 per Service Hour
Severe KPI Failure	>6 hours late, up to 12 hours late	105, then 1 per 3 minutes	>12 hours late, up to 24 hours late	130, then 1 per 6 minutes	>=3 Working Days late, up to 4 Working Days late	130, then 15 per Service Hour
KPI Service Threshold	>12 hours late	240, then 1 per 3 minutes	>24 hours late	250, then 1 per 6 minutes	>=4 Working Days late	250, then 15 per Service Hour

Service Credit Calculation

The Service Credit due in respect of KPI-05 is calculated in accordance with Paragraph 3.10 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing).

Severity 1 Security Incidents

The table below illustrates how different Security Incident Resolution Times for Severity 1 Security Incidents will result in differing numbers of Service Points and thus values of Service Credits due in that Service Period. For example, if a Severity 1 Security Incident is resolved 2 hours late, this would be a Minor KPI Failure, 44 Service Points would accrue and the Service Credits due would be:

Performance Indicators	Number of hours late in resolving the Security Incident	Service Points	Applicable percentage deduction	Fixed Service Charges and Volume Based Charges (£)	Service Credit Due (£)
		A	B	C	D A x B x C
Target Performance Level	0	0	0.01%		
Minor KPI Failure	2	44	0.01%		
Serious KPI Failure	4	74	0.01%		
Severe KPI Failure	9	165	0.01%		
KPI Service Threshold	18	360	0.01%		

Severity 2 Security Incidents

The table below illustrates how different Security Incident Resolution Times for Severity 2 Security Incidents will result in differing numbers of Service Points and thus values of Service Credits due in that Service Period. For example, if a Severity 2 Security Incident is resolved 8 hours late, this would be a Serious KPI Failure, 90 Service Points would accrue and the Service Credits due would be:

[REDACTED]

Performance Indicators	Number of hours late in responding to the Security Incident	Service Points	Applicable percentage deduction	Fixed Service Charges and Volume Based Charges (£)	Service Credit Due (£)
		<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i> <i>A x B x C</i>
Target Performance Level	0	0	0.01%		
Minor KPI Failure	2	30	0.01%		
Serious KPI Failure	8	90	0.01%		
Severe KPI Failure	18	190	0.01%		
KPI Service Threshold	30	310	0.01%		

Severity 3 Security Incidents

The table below illustrates how different Security Incident Resolution Times for Severity 3 Security Incidents will result in differing numbers of Service Points and thus values of Service Credits due in that Service Period. For example, if a Severity 3 Security Incident is resolved 13 hours (8 hours and 5 Service Hours) late, this would be a Minor KPI Failure, 35 Service Points would accrue and the Service Credits due would be:

[REDACTED]

Performance Indicators	Working Days and Service Hours late in responding to the Security Incident	Number of Service Hours late within the performance level band	Service Points	Applicable percentage deduction	Fixed Service Charges and Volume Based Charges (£)	Service Credit Due (£)
			<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i> <i>A x B x C</i>
Target Performance Level	0	0	0	0.01%		
Minor KPI Failure	8 hours and 5 Service Hours	5	35	0.01%		
Serious KPI Failure	2 Working Days and 2 Service Hours	2	70	0.01%		
Severe KPI Failure	3 Working Days and 4 Service Hours	4	190	0.01%		
KPI Service Threshold	4 Working Days and 6 Service Hours	6	340	0.01%		

Change Management KPI (KPI-06) - Service Credit Illustration

This worksheet provides, for information only, a Service Credit calculation example for the Change Management KPI (KPI-06) to illustrate how the provisions of Paragraph 3 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing) will be applied.

Assumptions

For the purpose of this example, the following assumptions have been made:

Item	Monthly Charges
Fixed Service Charges	[REDACTED]
Volume Based Charges	[REDACTED]
Fixed Service Charges and Volume Based Charges (£)	[REDACTED]

Service Point Accrual

The Service Points accrued in respect of KPI-06 are calculated in accordance with Paragraphs 1.1 of Part A and 5 of Part B of Annex 1 to Schedule 3 (Performance Levels).

Performance Indicators	< 100 Service Changes	> 99 Service Changes	Service Points
Target Performance Level	Up to one Failed Change	98%	0
Minor KPI Failure	Two Failed Changes	97% – 97.99%	10
Serious KPI Failure	Three Failed Changes	96.01% – 96.99%	20
Severe KPI Failure	Four Failed Changes	95.01% – 96%	30
KPI Service Threshold*	Five or more Failed Changes	Below 95.01%	40

*(1) Where there are fewer than 100 Service Changes within the Service Period, 10 additional Service Points for each additional Failed Change above the KPI Service Threshold

(2) Where there are 100 or more Service Changes within the Service Period, 10 additional Service Points for each percentage point below the KPI Service Threshold.

Service Credit Calculation

The Service Credit due in respect of KPI-06 is calculated in accordance with Paragraph 3.10 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing).

Where there are fewer than 100 Service Changes within the Service Period

are fewer than 100 Service Changes within a Service Period and 2 Failed Services Changes, then this would be a Minor KPI Failure, 10 Service Points would accrue and the Service Credits due would be:

Performance Indicators	Number of Failed Changes	Service Points	Applicable percentage deduction	Fixed Service Charges and Volume Based Charges (£)	Service Credit Due (£)
	A	B	C		D $A \times B \times C$
Target Performance Level	1	0	0.10%	[REDACTED]	[REDACTED]
Minor KPI Failure	2	10	0.10%	[REDACTED]	[REDACTED]
Serious KPI Failure	3	20	0.10%	[REDACTED]	[REDACTED]
Severe KPI Failure	4	30	0.10%	[REDACTED]	[REDACTED]
KPI Service Threshold	5	40	0.10%	[REDACTED]	[REDACTED]
KPI Service Threshold	7	60	0.10%	[REDACTED]	[REDACTED]

Where there are 100 or more Service Changes within the relevant Service Period

are 100 or more Service Changes within a Service Period with a Change Management % of 97.5%, then this would be a Minor KPI Failure, 10 Service Points would accrue and the Service Credits due would be:

[REDACTED]

Performance Indicators	Change Management %	Service Points	Applicable percentage deduction	Fixed Service Charges and Volume Based Charges (£)	Service Credit Due (£)
		<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i> <i>A x B x C</i>
Target Performance Level	98.50%	0	0.10%		[REDACTED]
Minor KPI Failure	97.50%	10	0.10%		
Serious KPI Failure	96.50%	20	0.10%		
Severe KPI Failure	95.50%	30	0.10%		
KPI Service Threshold	95.00%	40	0.10%		
KPI Service Threshold	93.00%	60	0.10%		

Service Request Fulfilment KPI (KPI-07) - Service Credit Illustration

This worksheet provides, for information only, a Service Credit calculation example for the Service Request Fulfilment KPI (KPI-07) to illustrate how the provisions of Paragraph 3 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing) will be applied.

Assumptions

For the purpose of this example, the following assumptions have been made:

Item	Monthly Charges
Fixed Service Charges	
Volume Based Charges	
Fixed Service Charges and Volume Based Charges (£)	

Service Point Accrual

The Service Points accrued in respect of KPI-07 are calculated in accordance with Paragraphs 1.1 of Part A and 6 of Part B of Annex 1 to Schedule 3 (Performance Levels).

Performance Indicators	< 100 Catalogue Items	> 99 Catalogue Items	Service Points
Target Performance Level	Up to one Late Catalogue Item	98%	0
Minor KPI Failure	Two Late Catalogue Items	97% – 97.99%	10
Serious KPI Failure	Three Late Catalogue Items	96.01% – 96.99%	20
Severe KPI Failure	Four Late Catalogue Items	95.01% – 96%	30
KPI Service Threshold*	Five or more Late Catalogue Items	Below 95.01%	40

*(1) Where fewer than 100 Catalogue Items were due to be achieved during the relevant Service Period, 10 additional Service Points for each additional Late Catalogue Item above the KPI Service Threshold
(2) Where 100 Catalogue Items or more were due to be achieved during the relevant Service Period, 10 additional Service Points for each percentage point below the KPI Service Threshold.

Service Credit Calculation

The Service Credit due in respect of KPI-07 is calculated in accordance with Paragraph 3.10 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing).

Where fewer than 100 Catalogue Items were due to be achieved during the Service Period

fewer than 100 Catalogue Items due to be achieved within a Service Period and 3 Late Catalogue Items, then this would be a Serious KPI Failure, 20 Service Points would accrue and the Service Credits due would be:

[REDACTED]

Performance Indicators	Number of Late Catalogue Items	Service Points	Applicable percentage deduction	Fixed Service Charges and Volume Based Charges (£)	Service Credit Due (£)
		A	B	C	D $A \times B \times C$
Target Performance Level	1	0	0.10%		
Minor KPI Failure	2	10	0.10%		
Serious KPI Failure	3	20	0.10%		
Severe KPI Failure	4	30	0.10%		
KPI Service Threshold	5	40	0.10%		
KPI Service Threshold	7	60	0.10%		

Where more than 99 Catalogue Items were due to be achieved during the Service Period

more Catalogue Items due to be achieved within a Service Period with a Service Request Fulfilment % of 96.5%, then this would be a Serious KPI Failure, 20 Service Points would accrue and the Service Credits due would be:

[REDACTED]

Performance Indicators	Service Request Fulfilment %	Service Points	Applicable percentage deduction	Fixed and Volumetric Service Charges (£)	Service Credit Due (£)
		A	B	C	D A x B x C
Target Performance Level	98.50%	0	0.10%		[REDACTED]
Minor KPI Failure	97.50%	10	0.10%		
Serious KPI Failure	96.50%	20	0.10%		
Severe KPI Failure	95.50%	30	0.10%		
KPI Service Threshold	95.00%	40	0.10%		
KPI Service Threshold	94.00%	50	0.10%		

Knowledge Management KPI (KPI-08) - Service Credit Illustration

This worksheet provides, for information only, a Service Credit calculation example for the Knowledge Management KPI (KPI-08) to illustrate how the provisions of Paragraph 3 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing) will be applied.

Assumptions

For the purpose of this example, the following assumptions have been made:

Item	Monthly Charges
Fixed Service Charges	
Volume Based Charges	
Fixed Service Charges and Volume Based Charges (£)	

Service Point Accrual

The Service Points accrued in respect of KPI-08 are calculated in accordance with Paragraphs 1.1 of Part A and 7 of Part B of Annex 1 to Schedule 3 (Performance Levels).

Performance Indicators	< 100 Knowledge Management Artefacts	> 99 Knowledge Management Artefacts	Service Points
Target Performance Level	Up to one Late Knowledge Management Artefact	98%	0
Minor KPI Failure	Two Late Knowledge Management Artefacts	97% – 97.99%	10
Serious KPI Failure	Three Late Knowledge Management Artefacts	96.01% – 96.99%	20
Severe KPI Failure	Four Late Knowledge Management Artefacts	95.01% – 96%	30
KPI Service Threshold*	Five or more Late Knowledge Management Artefacts	Below 95.01%	40

Threshold

(2) Where 100 or more Knowledge Management Artefacts are due to be created or updated during the relevant Service Period, 10 additional Service Points for each percentage point below the KPI Service Threshold.

Service Credit Calculation

The Service Credit due in respect of KPI-08 is calculated in accordance with Paragraph 3.10 of Part C (Adjustments to the Charges and Risk Register) of Schedule 15 (Charges and Invoicing).

Where fewer than 100 Catalogue Items were due to be achieved during the Service Period

Knowledge Management Artefacts due to be created or updated within a Service Period and 4 Late Knowledge Management Artefacts, then this would be a Severe KPI Failure, 30 Service Points would accrue and the Service Credits due would be:

[REDACTED]

Performance Indicators	Number of Late Knowledge Management Artefacts	Service Points	Applicable percentage deduction	Fixed Service Charges and Volume Based Charges (£)	Service Credit Due (£)
		A	B	C	D A x B x C
Target Performance Level	1	0	0.10%		
Minor KPI Failure	2	10	0.10%		
Serious KPI Failure	3	20	0.10%		
Severe KPI Failure	4	30	0.10%		
KPI Service Threshold	5	40	0.10%		
KPI Service Threshold	7	60	0.10%		

Where more than 99 Late Knowledge Management Artefact are due to be created or updated during the Service Period

The table below illustrates how different Late Knowledge Management % will result in differing numbers of Service Points and thus values of Service Credits due in that Service Period. For example, if there are 100 or more Knowledge Management Artefacts due to be created or updated within a Service Period with a Knowledge Management % of 95.5%, then this would be a Severe KPI Failure, 30 Service Points would accrue and the Service Credits due would be:

Performance Indicators	Knowledge Management %	Service Points	Applicable percentage deduction	Fixed Service Charges and Volume Based Charges (£)	Service Credit Due (£)
		A	B	C	D
Target Performance Level	98.50%	0	0.10%		
Minor KPI Failure	97.50%	10	0.10%		
Serious KPI Failure	96.50%	20	0.10%		
Severe KPI Failure	95.50%	30	0.10%		
KPI Service Threshold	95.00%	40	0.10%		
KPI Service Threshold	93.00%	60	0.10%		

SCHEDULE 16 (PAYMENTS ON TERMINATION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 16

PAYMENTS ON TERMINATION

SCHEDULE 16 (PAYMENTS ON TERMINATION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 16 (*Payments on Termination*)

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

“Applicable Supplier Personnel”

any Supplier Personnel who:

- (a) at the Termination Date:
 - (i) are employees of the Supplier;
 - (ii) are Dedicated Supplier Personnel;
 - (iii) have not transferred (and are not in scope to transfer at a later date) to the Authority or the Replacement Supplier by virtue of the Employment Regulations; and
- (b) are dismissed or given notice of dismissal by the Supplier within:
 - (i) 40 Working Days of the Termination Date; or
 - (ii) such longer period required by Law, their employment contract (as at the Termination Date) or an applicable collective agreement; and
- (c) have not resigned or given notice of resignation prior to the date of their dismissal by the Supplier; and
- (d) the Supplier can demonstrate to the satisfaction of the Authority:
 - (i) are surplus to the Supplier's requirements after the Termination Date notwithstanding its obligation to provide services to its other customers;
 - (ii) are genuinely being dismissed for reasons of redundancy; and
 - (iii) have been selected for redundancy by the Supplier on objective grounds other than the fact that the Supplier

SCHEDULE 16 (PAYMENTS ON TERMINATION)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

is entitled to reimbursement under this provision in respect of such employees;

“Breakage Costs Payment”	an amount equal to the Redundancy Costs and the Contract Breakage Costs as at the Termination Date as determined in accordance with Paragraph 3;
“Compensation Payment”	the payment calculated in accordance with Paragraph 6;
“Contract Breakage Costs”	the amounts payable by the Supplier to its Key Sub-contractors or other third parties (as applicable) for terminating all relevant Key Sub-contracts or Third Party Contracts as a direct result of the early termination of this Contract;
“Dedicated Supplier Personnel”	all Supplier Personnel then assigned to the Services or any part of the Services. If the Supplier is unsure as to whether Supplier Personnel are or should be regarded as so assigned, it shall consult with the Authority whose view shall be determinative provided that the employee has been materially involved in the provision of the Services or any part of the Services;
“Profit Already Paid”	the Supplier Profit paid or payable to the Supplier under this Contract for the period from the Effective Date up to (and including) the Termination Date;
“Redundancy Costs”	the total sum of any of the following sums paid to Applicable Supplier Personnel, each amount apportioned between the Supplier and the Authority based on the time spent by such employee on the Services as a proportion of the total Service duration: (a) any statutory redundancy payment; and (b) in respect of an employee who was a Transferring Former Supplier Employee or a Transferring Authority Employee, any contractual redundancy payment (or where such a contractual benefit on redundancy is a benefit payable from a pension scheme, the increase in cost to the Supplier as a net present value compared to the benefit

SCHEDULE 16 (PAYMENTS ON TERMINATION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

payable on termination of employment without redundancy), provided that such employee was entitled to such contractual redundancy payment immediately prior to his or her transfer to the Supplier under the Employment Regulations;

“Request for Estimate”

a written request sent by the Authority to the Supplier, requiring that the Supplier provide it with an accurate estimate of the Termination Payment and Compensation Payment that would be payable if the Authority exercised its right under Clause 31.1(a) (*Termination by the Authority*) to terminate this Contract for convenience on a specified Termination Date;

“Shortfall Period”

has the meaning given in Paragraph 6.2;

“Termination Estimate”

has the meaning given in Paragraph 11.2;

“Third Party Contract”

a contract with a third party entered into by the Supplier exclusively for the purpose of delivering the Services, as listed in Schedule 11 (Third Party Contracts);

“Total Costs Incurred”

the Costs incurred by the Supplier up to the Termination Date in the performance of this Contract and detailed in the Financial Model (but excluding Contract Breakage Costs, Redundancy Costs and any costs the Supplier would not otherwise be able to recover through the Charges) less any Deductions up to (and including) the Termination Date;

“Unrecovered Costs”

the Costs incurred by the Supplier in the performance of this Contract (as summarised in the Financial Model) to the extent that the same remain at the Termination Date to be recovered through Charges that but for the termination of this Contract would have been payable by the Authority after the Termination Date in accordance with as such Costs and Charges are forecast in the Financial Model;

“Unrecovered Payment”

an amount equal to the lower of:

SCHEDULE 16 (PAYMENTS ON TERMINATION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (a) the sum of the Unrecovered Costs and the Unrecovered Profit; and
- (b) the amount specified in Paragraph 4; and

“Unrecovered Profit” (Total Costs Incurred x Anticipated Contract Life Profit Margin) - Profit Already Paid + Milestone Retentions remaining unpaid at the Termination Date.

2 TERMINATION PAYMENT

- 2.1 The Termination Payment payable pursuant to Clause 32.3(a) (*Payments by the Authority*) shall be an amount equal to the aggregate of the Breakage Costs Payment and the Unrecovered Payment.

3 BREAKAGE COSTS PAYMENT

- 3.1 The Supplier may recover through the Breakage Costs Payment only those costs incurred by the Supplier directly as a result of the termination of this Contract which:
 - (a) would not have been incurred had this Contract continued until expiry of the Initial Term, or in the event that the Term has been extended, the expiry of the Extension Period;
 - (b) are unavoidable, proven, reasonable, and not capable of recovery;
 - (c) are incurred under arrangements or agreements that are directly associated with this Contract;
 - (d) are not Contract Breakage Costs relating to contracts or Sub-contracts with Affiliates of the Supplier; and
 - (e) relate directly to the termination of the Services.

Limitation on Breakage Costs Payment

- 3.2 The Breakage Costs Payment shall not exceed the lower of:
 - (a) the relevant limit set out in Annex 1; and
 - (b) 120% of the estimate for the Breakage Costs Payment set out in any relevant Termination Estimate.

Redundancy Costs

- 3.3 The Authority shall not be liable under this Schedule for any costs associated with Supplier Personnel (whether relating to redundancy, redeployment or otherwise) other than the Redundancy Costs.
- 3.4 Where the Supplier can demonstrate that a member of Supplier Personnel will be made redundant following termination of this Contract, but redeployment of

SCHEDULE 16 (PAYMENTS ON TERMINATION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

such person is possible and would offer value for money to the Authority when compared with redundancy, then the Authority shall pay the Supplier the actual direct costs incurred by the Supplier or its Sub-contractor arising out of the redeployment of such person (including retraining and relocation costs) subject to a maximum amount of £30,000 per relevant member of the Supplier Personnel.

Contract Breakage Costs

- 3.5 The Supplier shall be entitled to Contract Breakage Costs only in respect of Third Party Contracts or Sub-contracts which:
- (a) are not assigned or novated to a Replacement Supplier at the request of the Authority in accordance with Schedule 25 (*Exit Management*); and
 - (b) the Supplier can demonstrate:
 - (i) are surplus to the Supplier's requirements after the Termination Date, whether in relation to use internally within its business or in providing services to any of its other customers; and
 - (ii) have been entered into by it in the ordinary course of business.
- 3.6 The Supplier shall seek to negotiate termination of any Third Party Contracts or Sub-contracts with the relevant third party or Sub-contractor (as the case may be) using all reasonable endeavours to minimise the cancellation or termination charges.
- 3.7 Except with the prior written agreement of the Authority, the Authority shall not be liable for any costs (including cancellation or termination charges) that the Supplier is obliged to pay in respect of:
- (a) the termination of any contractual arrangements for occupation of, support of and/or services provided for Supplier premises which may arise as a consequence of the termination of this Contract; and/or
 - (b) Assets not yet installed at the Termination Date.

4 UNRECOVERED PAYMENT

The Unrecovered Payment shall not exceed the lowest of:

- (a) the relevant limit set out in Annex 1;
- (b) 120% of the estimate for the Unrecovered Payment set out in any relevant Termination Estimate; and
- (c) the Charges that but for the termination of this Contract would have been payable by the Authority after the Termination Date in

SCHEDULE 16 (PAYMENTS ON TERMINATION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

accordance with Schedule 15 (*Charges and Invoicing*) as forecast in the Financial Model.

5 MITIGATION OF CONTRACT BREAKAGE COSTS, REDUNDANCY COSTS AND UNRECOVERED COSTS

- 5.1 The Supplier agrees to use all reasonable endeavours to minimise and mitigate Contract Breakage Costs, Redundancy Costs and Unrecovered Costs by:
- (a) the appropriation of Assets, employees and resources for other purposes;
 - (b) at the Authority's request, assigning any Third Party Contracts and Sub-contracts to the Authority or a third party acting on behalf of the Authority; and
 - (c) in relation Third Party Contracts and Sub-contract that are not to be assigned to the Authority or to another third party, terminating those contracts at the earliest possible date without breach or where contractually permitted.
- 5.2 If Assets, employees and resources can be used by the Supplier for other purposes, then there shall be an equitable reduction in the Contract Breakage Costs, Redundancy Costs and Unrecovered Costs payable by the Authority or a third party to the Supplier. In the event of any Dispute arising over whether the Supplier can use any Assets, employees and/or resources for other purposes and/or over the amount of the relevant equitable reduction, the Dispute shall be referred to an Expert for determination in accordance with the procedure detailed in Schedule 23 (*Dispute Resolution Procedure*).

6 COMPENSATION PAYMENT

- 6.1 The Compensation Payment payable pursuant to Clause 32.3(b) (*Payments by the Authority*) shall be an amount equal to the total forecast Charges over the Shortfall Period (as stated in the Financial Model) multiplied by the Anticipated Contract Life Profit Margin.
- 6.2 For the purposes of Paragraph 6.1, the "**Shortfall Period**" means:
- (a) where the Authority terminates this Contract pursuant to Clause 31.1(a) (*Termination by the Authority*), a number of days equal to the number of days by which the notice given (or deemed given pursuant to Paragraph 2.1(a) Part D of Schedule 15 (*Charges and Invoicing*)) falls short of three hundred and sixty-five (365) days; or
 - (b) where the Supplier terminates this Contract pursuant to Clause 31.3(a) (*Termination by the Supplier*), a number of days equal to the number of days by which the period from (and including) the date of the non-payment by the Authority to (and including) the Termination Date falls short of 365 days,

SCHEDULE 16 (PAYMENTS ON TERMINATION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

but in each case subject to the limit set out in Paragraph 6.3.

6.3 The Compensation Payment shall be no greater than the lower of:

- (a) the relevant limit set out in Annex 1; and
- (b) 120% of the estimate for the Compensation Payment set out in the relevant Termination Estimate.

7 FULL AND FINAL SETTLEMENT

7.1 Any Termination Payment and/or Compensation Payment paid under this Schedule shall be in full and final settlement of any claim, demand and/or proceedings of the Supplier in relation to any termination by the Authority pursuant to Clause 31.1(a) (*Termination by the Authority*) or termination by the Supplier pursuant to Clause 31.3(a) (*Termination by the Supplier*) (as applicable), and the Supplier shall be excluded from all other rights and remedies it would otherwise have been entitled to in respect of any such termination.

8 INVOICING FOR THE PAYMENTS ON TERMINATION

8.1 All sums due under this Schedule shall be payable by the Authority to the Supplier in accordance with the payment terms set out in Schedule 15 (*Charges and Invoicing*).

9 SET OFF

9.1 The Authority shall be entitled to set off any outstanding liabilities of the Supplier against any amounts that are payable by it pursuant to this Schedule.

10 NO DOUBLE RECOVERY

10.1 If any amount payable under this Schedule (in whole or in part) relates to or arises from any Transferring Assets then, to the extent that the Authority makes any payments pursuant to Schedule 25 (*Exit Management*) in respect of such Transferring Assets, such payments shall be deducted from the amount payable pursuant to this Schedule.

10.2 The value of the Termination Payment and/or the Compensation Payment shall be reduced or extinguished to the extent that the Supplier has already received the Charges or the financial benefit of any other rights or remedy given under this Contract including the payment of any Annual Shortfall Payment in accordance with Paragraph 4.3.5 of Part A (Pricing) of Schedule 15 (*Charges and Invoicing*), so that there is no double counting in calculating the relevant payment.

10.3 Any payments that are due in respect of the Transferring Assets shall be calculated in accordance with the provisions of the Exit Plan.

SCHEDULE 16 (PAYMENTS ON TERMINATION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

11 ESTIMATE OF TERMINATION PAYMENT AND COMPENSATION PAYMENT

- 11.1 The Authority may issue a Request for Estimate at any time during the Term provided that no more than 2 Requests for Estimate may be issued in any 6 month period.
- 11.2 The Supplier shall within 20 Working Days of receiving the Request for Estimate (or such other timescale agreed between the Parties), provide an accurate written estimate of the Termination Payment and the Compensation Payment that would be payable by the Authority based on a postulated Termination Date specified in the Request for Estimate (such estimate being the "**Termination Estimate**"). The Termination Estimate shall:
- (a) be based on the relevant amounts set out in the Financial Model;
 - (b) include:
 - (i) details of the mechanism by which the Termination Payment is calculated;
 - (ii) full particulars of the estimated Contract Breakage Costs in respect of each Sub-contract or Third Party Contract and appropriate supporting documentation; and
 - (iii) such information as the Authority may reasonably require; and
 - (c) state the period for which that Termination Estimate remains valid, which shall be not less than 20 Working Days.
- 11.3 The Supplier acknowledges that issue of a Request for Estimate shall not be construed in any way as to represent an intention by the Authority to terminate this Contract.
- 11.4 If the Authority issues a Termination Notice to the Supplier within the stated period for which a Termination Estimate remains valid, the Supplier shall use the same mechanism to calculate the Termination Payment as was detailed in the Termination Estimate unless otherwise agreed in writing between the Supplier and the Authority.

SCHEDULE 16 (PAYMENTS ON TERMINATION)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 1: MAXIMUM PAYMENTS ON TERMINATION

The table below sets out, by Contract Year, the maximum amount of the Unrecovered Payment, Breakage Costs Payment and Compensation Payment that the Authority shall be liable to pay to the Supplier pursuant to this Contract:

Termination Date	Maximum Unrecovered Payment	Maximum Breakage Costs Payment	Maximum Compensation Payment
Anytime in the first Contract Year	[REDACTED]	[REDACTED]	[REDACTED]
Anytime in the second Contract Year	[REDACTED]	[REDACTED]	[REDACTED]
Anytime in Contract Year 3	[REDACTED]	[REDACTED]	[REDACTED]
Anytime in Contract Year 4	[REDACTED]	[REDACTED]	[REDACTED]
Anytime in Contract Year 5	[REDACTED]	[REDACTED]	[REDACTED]
Anytime in Contract Year 6	[REDACTED]	[REDACTED]	[REDACTED]
Anytime in Contract Year 7	[REDACTED]	[REDACTED]	[REDACTED]
Anytime during the optional Extension Period (Contract Years 8 – 10)	[REDACTED]	[REDACTED]	[REDACTED]

SCHEDULE 17 (BENCHMARKING)
Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SCHEDULE 17

BENCHMARKING

SCHEDULE 17 (BENCHMARKING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 17 (*Benchmarking*)

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

“Benchmarked Service”	a Service that the Authority elects to include in a Benchmark Review under Paragraph 2.3;
“Benchmarker”	the independent third party appointed under Paragraph 3.1;
“Benchmark Report”	the report produced by the Benchmarker following the Benchmark Review as further described in Paragraph 5;
“Benchmark Review”	a review of one or more of the Services carried out in accordance with Paragraph 4 to determine whether those Services represent Good Value;
“Comparable Service”	in relation to a Benchmarked Service, a service that is identical or materially similar to the Benchmarked Service (including in terms of scope, specification, volume and quality of performance);
“Comparison Group”	in relation to a Comparable Service, a sample group of organisations providing the Comparable Service identified by the Benchmarker under Paragraph 4.8 which consists of organisations which are either of similar size to the Supplier or which are similarly structured in terms of their business and their service offering so as to be (in the Benchmarker's professional opinion) fair comparators with the Supplier or which, in the professional opinion of the Benchmarker, are best practice organisations and, where there are a reasonable number of such organisations, referencing only those organisations that are carrying on at least a significant part of their business within the United Kingdom;
“Equivalent Services Data”	in relation to a Comparable Service, data derived from an analysis of the Comparable Service provided by the Comparison Group as adjusted in accordance with Paragraphs 4.8(a) and 4.9 provided that the Benchmarker shall not use any such data that relates to a period which ended

SCHEDULE 17 (BENCHMARKING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

more than 36 months prior to the date of the appointment of the Benchmarker;

“Good Value”

in relation to a Benchmarked Service, that:

- (a) having taken into account the Performance Indicators and Target Service Levels, the value for money of the Charges attributable to that Benchmarked Service is at least as good as the value for money of the Upper Quartile; and
- (b) any Performance Indicators and Target Service Levels applicable to that Benchmarked Service are, having taken into account the Charges, equal to or better than the median service levels for the Comparable Service using Equivalent Services Data; and

“Upper Quartile”

the top 25% of instances of provision of a Comparable Service by members of the Comparison Group ranked by best value for money to the recipients of that Comparable Service.

2 FREQUENCY, PURPOSE AND SCOPE OF BENCHMARK REVIEW

- 2.1 The Authority may, by written notice to the Supplier, require a Benchmark Review of any or all of the Services in order to establish whether a Benchmarked Service is, and/or the Benchmarked Services as a whole are, Good Value.
- 2.2 The Authority shall be entitled to carry out Benchmark Review(s) of any Services following the second anniversary of the First Operational Service Commencement Date for those Services).
- 2.3 The Services that are to be the Benchmarked Services shall be identified by the Authority in the notice given under Paragraph 2.1.

3 APPOINTMENT OF BENCHMARKER

- 3.1 The Authority shall appoint as the Benchmarker to carry out the Benchmark Review either an organisation on the list of organisations set out in Annex 1 or such other organisation as may be agreed in writing between the Parties.
- 3.2 The Authority shall, at the written request of the Supplier, require the Benchmarker to enter into a confidentiality agreement with the Supplier in, or substantially in, the form set out in Annex 2.

SCHEDULE 17 (BENCHMARKING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

3.3 The costs and expenses of the Benchmarker and the Benchmark Review shall be shared equally between both Parties provided that each Party shall bear its own internal costs of the Benchmark Review. The Benchmarker shall not be compensated on a contingency fee or incentive basis.

3.4 The Authority shall be entitled to pay the Benchmarker's costs and expenses in full and to recover the Supplier's share from the Supplier.

4 BENCHMARK REVIEW

4.1 The Authority shall require the Benchmarker to produce, and to send to each Party for approval, a draft plan for the Benchmark Review within 10 Working Days after the date of the appointment of the Benchmarker, or such longer period as the Benchmarker shall reasonably request in all the circumstances. The plan must include:

- (a) a proposed timetable for the Benchmark Review;
- (b) a description of the information that the Benchmarker requires each Party to provide;
- (c) a description of the benchmarking methodology to be used;
- (d) a description that clearly illustrates that the benchmarking methodology to be used is capable of fulfilling the benchmarking objectives under Paragraph 2.1;
- (e) an estimate of the resources required from each Party to underpin the delivery of the plan;
- (f) a description of how the Benchmarker will scope and identify the Comparison Group;
- (g) details of any entities which the Benchmarker proposes to include within the Comparison Group; and
- (h) if in the Benchmarker's professional opinion there are no Comparable Services or the number of entities carrying out Comparable Services is insufficient to create a Comparison Group, a detailed approach for meeting the relevant benchmarking objective(s) under Paragraph 2.1 using a proxy for the Comparison Services and/or Comparison Group as applicable.

4.2 The Parties acknowledge that the selection and or use of proxies for the Comparison Group (both in terms of number and identity of entities) and Comparable Services shall be a matter for the Benchmarker's professional judgment.

4.3 Each Party shall give notice in writing to the Benchmarker and to the other Party within 10 Working Days after receiving the draft plan either approving the draft plan or suggesting amendments to that plan which must be reasonable. Where a Party suggests amendments to the draft plan pursuant to this Paragraph 4.3, the Benchmarker shall, if it believes the amendments

SCHEDULE 17 (BENCHMARKING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

are reasonable, produce an amended draft plan. Paragraph 4.1 and this Paragraph 4.3 shall apply to any amended draft plan.

- 4.4 Failure by a Party to give notice under Paragraph 4.3 shall be treated as approval of the draft plan by that Party. If the Parties fail to approve the draft plan within 30 Working Days of its first being sent to them pursuant to Paragraph 4.1 then the Benchmarker shall prescribe the plan.
- 4.5 Once the plan is approved by both Parties or prescribed by the Benchmarker, the Benchmarker shall carry out the Benchmark Review in accordance with the plan. Each Party shall procure that all the information described in the plan, together with any additional information reasonably required by the Benchmarker is provided to the Benchmarker without undue delay. If the Supplier fails to provide any information requested from it by the Benchmarker and described in the plan, such failure shall constitute a material Default for the purposes of Clause 25.1(c) (*Rectification Plan Process*).
- 4.6 Each Party shall co-operate fully with the Benchmarker, including by providing access to records, technical documentation, premises, equipment, systems and personnel at times reasonably requested by the Benchmarker, provided that the Benchmarker shall be instructed to minimise any disruption to the Services.
- 4.7 Either Party may provide additional material to the Benchmarker to assist the Benchmarker in conducting the Benchmark Review.
- 4.8 Once it has received the information it requires, the Benchmarker shall:
- (a) finalise the sample of entities constituting the Comparison Group and collect data relating to Comparable Services. The final selection of the Comparison Group (both in terms of number and identity of entities) and of the Comparable Services shall be a matter for the Benchmarker's professional judgment;
 - (b) derive the Equivalent Services Data by applying the adjustment factors listed in Paragraph 4.9 and from an analysis of the Comparable Services;
 - (c) derive the relative value for money of the charges payable for the Comparable Services using the Equivalent Services Data and from that derive the Upper Quartile;
 - (d) derive the median service levels relating to the Comparable Services using the Equivalent Services Data;
 - (e) compare the value for money of the Charges attributable to the Benchmarked Services (having regard in particular to the applicable Performance Indicators and Target Service Levels) to the value for money of the Upper Quartile;
 - (f) compare the Performance Indicators and Target Service Levels attributable to the Benchmarked Services (having regard to the

SCHEDULE 17 (BENCHMARKING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Charges and Service Credits) with the median service levels using the Equivalent Services Data; and

- (g) determine whether or not each Benchmarked Service is and/or the Benchmarked Services as a whole are, Good Value.

4.9 The Benchmarker shall have regard to the following matters when performing a comparative assessment of a Benchmarked Service and a Comparable Service in order to derive Equivalent Services Data:

- (a) the contractual and business environment under which the Services are being provided (including the scope, scale, complexity and geographical spread of the Services);
- (b) any front-end investment and development costs of the Supplier;
- (c) the Supplier's risk profile including the financial, performance or liability risks associated with the provision of the Services as a whole;
- (d) the extent of the Supplier's management and contract governance responsibilities;
- (e) any other reasonable factors demonstrated by the Supplier, which, if not taken into consideration, could unfairly cause the Supplier's pricing to appear non-competitive (such as erroneous costing, non-sustainable behaviour including excessive consumption of energy or over-aggressive pricing).

5 BENCHMARK REPORT

5.1 The Benchmarker shall be required to prepare a Benchmark Report and deliver it simultaneously to both Parties, at the time specified in the plan approved under Paragraph 4, setting out its findings. The Benchmark Report shall:

- (a) include a finding as to whether or not each Benchmarked Service is and/or whether the Benchmarked Services as a whole are, Good Value;
- (b) include other findings (if any) regarding the quality and competitiveness or otherwise of those Services;
- (c) if any Benchmarked Service is not Good Value, or the Benchmarked Services as a whole are not Good Value, specify the changes that would be required to the Charges, Performance Indicators and/or Target Performance Levels, that would be required to make that Benchmarked Service or those Benchmarked Services as a whole Good Value; and
- (d) illustrate the method used for any normalisation of the Equivalent Services Data

SCHEDULE 17 (BENCHMARKING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 5.2 The Benchmarker shall act as an expert and not as an arbitrator.
- 5.3 If the Benchmark Report states that any Benchmarked Service is not Good Value or that the Benchmarked Services as a whole are not Good Value, then the Supplier shall (subject to Paragraphs 5.5 and 5.6) implement the changes set out in the Benchmark Report as soon as reasonably practicable within timescales agreed with the Authority but in any event within no more than 3 months. Any associated changes to the Charges shall take effect only from the same date and shall not be retrospective.
- 5.4 The Supplier acknowledges and agrees that Benchmark Reviews shall not result in any increase to the Charges, disapplication of the Performance Indicators or any reduction in the Target Performance Levels.
- 5.5 The Supplier shall be entitled to reject any Benchmark Report if the Supplier reasonably considers that the Benchmarker has not followed the procedure for the related Benchmark Review as set out in this Schedule in any material respect.
- 5.6 The Supplier shall not be obliged to implement any Benchmark Report to the extent this would cause the Supplier to provide the Services at a loss (as determined, by reference to the Financial Model), or to the extent the Supplier cannot technically implement the recommended changes.
- 5.7 In the event of any Dispute arising over whether the Benchmarker has followed the procedure for the related Benchmark Review under Paragraph 5.5 and/or any matter referred to in Paragraph 5.6, the Dispute shall be referred to Expert Determination. For the avoidance of doubt in the event of a Dispute between the Parties, the Authority shall continue to pay the Charges to the Supplier in accordance with the terms of this Contract and the Performance Indicators and Target Performance Levels shall remain unchanged pending the conclusion of the Expert Determination.
- 5.8 On conclusion of the Expert Determination:
- (a) if the Expert determines that all or any part of the Benchmark Report recommendations regarding any reduction in the Charges shall be implemented by the Supplier, the Supplier shall immediately repay to the Authority the difference between the Charges paid by the Authority up to and including the date of the Expert's determination and the date upon which the recommended reduction in Charges should have originally taken effect pursuant to Paragraph 5.3 together with interest thereon at the applicable rate under the Late Payment Of Commercial Debts (Interest) Act 1998; and
 - (b) if the Expert determines that all or any part of the Benchmark Report recommendations regarding any changes to the Performance Indicators and/or Target Performance Levels shall be implemented by the Supplier:

SCHEDULE 17 (BENCHMARKING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (i) the Supplier shall immediately implement the relevant changes;
- (ii) the Supplier shall immediately pay an amount equal to any Service Credits which would have accrued up to and including the date of the Expert's determination if the relevant changes had taken effect on the date determined pursuant to Paragraph 5.3 together with interest thereon at the applicable rate under the Late Payment Of Commercial Debts (Interest) Act 1998; and
- (iii) the relevant changes shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment for the purposes of this Contract.

5.9 Any failure by the Supplier to implement the changes as set out in the Benchmark Report in accordance with the relevant timescales determined in accordance with Paragraph 5.3 (unless the provisions of Paragraph 5.6 and/or Paragraph 5.7 apply) or in accordance with Paragraph 5.8 shall, without prejudice to any other rights or remedies of the Authority, constitute a Supplier Termination Event.

SCHEDULE 17 (BENCHMARKING)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 1: APPROVED BENCHMARKERS

Organisations Name	Address
[REDACTED]	

SCHEDULE 17 (BENCHMARKING)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [redacted]

ANNEX 2: CONFIDENTIALITY AGREEMENT

CONFIDENTIALITY AGREEMENT

THIS AGREEMENT is made on [date]

BETWEEN:

- (1) [insert name] of [insert address] (the “Supplier”); and
- (2) [insert name] of [insert address] (the “Benchmarker” and together with the Supplier, the “Parties”).

WHEREAS:

- (A) Secretary of State for Justice (the “Authority”) and the Supplier are party to a contract dated [insert date] (the “Contract”) for the provision by the Supplier of WAN Services to the Authority.
- (B) The Benchmarker is to receive Confidential Information from the Supplier for the purpose of carrying out a benchmarking review for the Authority of one or more of such services pursuant to the terms of the Contract (the “Permitted Purpose”).

IT IS AGREED as follows:

1 Interpretation

1.1 In this Agreement, unless the context otherwise requires:

“Confidential Information”

means:

- (a) Information, including all personal data within the meaning of the Data Protection Act 2018, and however it is conveyed, provided by the Supplier to the Benchmarker pursuant to this Agreement that relates to:
 - (i) the Supplier; or
 - (ii) the operations, business, affairs, developments, intellectual property rights, trade secrets, know-how and/or personnel of the Supplier;
- (b) other Information provided by the Supplier pursuant to this Agreement to the Benchmarker that is clearly designated as being confidential or equivalent or that ought reasonably to be considered to be confidential which comes (or has come) to

SCHEDULE 17 (BENCHMARKING)

Confidential
 Contract for the provision of WAN Services

Security Classification (Official)
 Contract reference: [REDACTED]

the Benchmarker’s attention or into the Benchmarker’s possession in connection with the Permitted Purpose;

- (c) discussions, negotiations, and correspondence between the Supplier or any of its directors, officers, employees, consultants or professional advisers and the Benchmarker or any of its directors, officers, employees, consultants and professional advisers in connection with the Permitted Purpose and all matters arising therefrom; and
- (d) Information derived from any of the above, but not including any Information that:
- (e) was in the possession of the Benchmarker without obligation of confidentiality prior to its disclosure by the Supplier;
- (f) the Benchmarker obtained on a non-confidential basis from a third party who is not, to the Benchmarker’s knowledge or belief, bound by a confidentiality agreement with the Supplier or otherwise prohibited from disclosing the information to the Benchmarker;
- (g) was already generally available and in the public domain at the time of disclosure otherwise than by a breach of this Agreement or breach of a duty of confidentiality; or
- (h) was independently developed without access to the Confidential Information;

“Information” means all information of whatever nature, however conveyed and in whatever form, including in writing, orally, by demonstration, electronically and in a tangible, visual or machine-readable medium (including CD-ROM, magnetic and digital form); and

“Permitted Purpose” has the meaning given to that expression in recital (B) to this Agreement.

SCHEDULE 17 (BENCHMARKING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

1.2 In this Agreement:

- (a) a reference to any gender includes a reference to other genders;
- (b) the singular includes the plural and vice versa;
- (c) the words "include" and cognate expressions shall be construed as if they were immediately followed by the words "without limitation";
- (d) references to any statutory provision include a reference to that provision as modified, replaced, amended and/or re-enacted from time to time (before or after the date of this Agreement) and any prior or subsequent subordinate legislation made under it;
- (e) headings are included for ease of reference only and shall not affect the interpretation or construction of this Agreement; and
- (f) references to Clauses are to clauses of this Agreement.

2 Confidentiality Obligations**2.1 In consideration of the Supplier providing Confidential Information to the Benchmark, the Benchmark shall:**

- (a) treat all Confidential Information as secret and confidential;
- (b) have in place and maintain proper security measures and procedures to protect the confidentiality of the Confidential Information (having regard to its form and nature);
- (c) not disclose or permit the disclosure of any of the Confidential Information to any other person without obtaining the prior written consent of the Supplier or, if relevant, other owner or except as expressly set out in this Agreement;
- (d) not transfer any of the Confidential Information outside the United Kingdom;
- (e) not use or exploit any of the Confidential Information for any purpose whatsoever other than the Permitted Purpose;
- (f) immediately notify the Supplier in writing if it suspects or becomes aware of any unauthorised access, copying, use or disclosure in any form of any of the Confidential Information; and
- (g) once the Permitted Purpose has been fulfilled:
 - (i) destroy or return to the Supplier all documents and other tangible materials that contain any of the Confidential Information;
 - (ii) ensure, so far as reasonably practicable, that all Confidential Information held in electronic, digital or other machine-readable form ceases to be readily accessible (other than by

SCHEDULE 17 (BENCHMARKING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

the information technology staff of the Benchmarker) from any computer, word processor, voicemail system or any other device; and

(iii) make no further use of any Confidential Information.

3 Permitted Disclosures

3.1 The Benchmarker may disclose Confidential Information to those of its directors, officers, employees, consultants and professional advisers who:

- (a) reasonably need to receive the Confidential Information in connection with the Permitted Purpose; and
- (b) have been informed by the Benchmarker of the confidential nature of the Confidential Information; and
- (c) have agreed to terms similar to those in this Agreement.

3.2 The Benchmarker shall be entitled to disclose Confidential Information to the Authority for the Permitted Purpose and to any Expert appointed in relation to a Dispute as referred to in Paragraph 5.7 of this

SCHEDULE 17 (BENCHMARKING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 3.3 Schedule 17 (*Benchmarking*) to the Contract.
- 3.4 The Benchmarker shall be entitled to disclose Confidential Information to the extent that it is required to do so by applicable law or by order of a court or other public body that has jurisdiction over the Benchmarker.
- 3.5 Before making a disclosure pursuant to Clause 3.4, the Benchmarker shall, if the circumstances permit:
- (a) notify the Supplier in writing of the proposed disclosure as soon as possible (and if possible before the court or other public body orders the disclosure of the Confidential Information); and
 - (b) ask the court or other public body to treat the Confidential Information as confidential.

4 General

- 4.1 The Benchmarker acknowledges and agrees that all property, including intellectual property rights, in Confidential Information disclosed to it by the Supplier shall remain with and be vested in the Supplier.
- 4.2 This Agreement does not include, expressly or by implication, any representations, warranties or other obligations:
- (a) to grant the Benchmarker any licence or rights other than as may be expressly stated in this Agreement;
 - (b) to require the Supplier to disclose, continue disclosing or update any Confidential Information; or
 - (c) as to the accuracy, efficacy, completeness, capabilities, safety or any other qualities whatsoever of any Information or materials provided pursuant to or in anticipation of this Agreement.
- 4.3 The rights, powers and remedies provided in this Agreement are cumulative and not exclusive of any rights, powers or remedies provided by law. No failure or delay by either Party to exercise any right, power or remedy will operate as a waiver of it nor will any partial exercise preclude any further exercise of the same, or of some other right, power or remedy.
- 4.4 Without prejudice to any other rights or remedies that the Supplier may have, the Benchmarker acknowledges and agrees that damages alone may not be an adequate remedy for any breach by the Benchmarker of any of the provisions of this Agreement. Accordingly, the Benchmarker acknowledges that the Supplier shall be entitled to the remedies of injunction and specific performance as well as any other equitable relief for any threatened or actual breach of this Agreement and/or breach of confidence and that no proof of special damages shall be necessary for the enforcement of such remedies.
- 4.5 The maximum liability of the Benchmarker to the Supplier for any breach of this Agreement shall be limited to ten million pounds (£10,000,000).

SCHEDULE 17 (BENCHMARKING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 4.6 For the purposes of the Contracts (Rights of Third Parties) Act 1999 no one other than the Parties has the right to enforce the terms of this Agreement.
- 4.7 Each Party shall be responsible for all costs incurred by it or on its behalf in connection with this Agreement.
- 4.8 This Agreement may be executed in any number of counterparts and by the Parties on separate counterparts, but shall not be effective until each Party has executed at least one counterpart. Each counterpart shall constitute an original of this Agreement, but all the counterparts shall together constitute but one and the same instrument.

5 Notices

- 5.1 Any notice to be given under this Agreement (each a “**Notice**”) shall be given in writing and shall be delivered by hand and shall be deemed to have been duly given at the time of delivery provided that such Notice is sent to the relevant physical address, and expressly marked for the attention of the relevant individual, set out in Clause 5.2.

- 5.2 Any Notice:

- (a) if to be given to the Supplier shall be sent to:

[Address]

Attention: [Contact name and/or position, e.g. “The Finance Director”]

- (b) if to be given to the Benchmarkers shall be sent to:

[Name of Organisation]

[Address]

Attention: [REDACTED]

6 Governing law

- 6.1 This Agreement shall be governed by, and construed in accordance with, English law and any matter claim or dispute arising out of or in connection with this Agreement whether contractual or non-contractual, shall be governed by and determined in accordance with English law.
- 6.2 Each Party hereby irrevocably submits to the exclusive jurisdiction of the English courts in respect of any claim or dispute arising out of or in connection with this Agreement.

IN WITNESS of the above this Agreement has been signed by the duly authorised representatives of the Parties on the date which appears at the head of page 1.

For and on behalf of [name of Supplier]

SCHEDULE 17 (BENCHMARKING)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Signature: _____

Date:

Name:

Position:

For and on behalf of **[*name of Benchmark*er]**

Signature: _____

Date:

Name:

Position:

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 18

FINANCIAL DISTRESS

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 18 (*Financial Distress*)

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

“Applicable Financial Indicators”	means the financial indicators from Paragraph 5.1 of this Schedule which are to apply to the Monitored Suppliers as set out in Paragraph 5.2 of this Schedule;
“Board”	means the Supplier's board of directors;
“Board Confirmation”	means written confirmation from the Board in accordance with Paragraph 8 of this Schedule;
“Credit Rating Level”	a credit rating level as specified in Annex 1 of this Schedule;
“Credit Rating Threshold”	the minimum Credit Rating Level for each entity in the FDE Group as set out in Annex 2 of this Schedule;
“FDE Group”	means the Supplier, Key Sub-contractors, and the Monitored Suppliers;
“Financial Indicators”	in respect of the Supplier and Key Sub-contractors, means each of the financial indicators set out at Paragraph 5.1 of this Schedule; and in respect of each Monitored Supplier, means those Applicable Financial Indicators;
“Financial Target Thresholds”	means the target thresholds for each of the Financial Indicators set out at Paragraph 5.1 of this Schedule;
“FVRA”	means a financial viability and risk assessment in the form completed by the Supplier as part of its Selection Questionnaire response;
“Monitored Suppliers”	means those entities specified at Paragraph 5.2 of this Schedule;
“Rating Agencies”	the rating agencies listed in Annex 1 of this Schedule.

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 1.2 For the purposes of this Schedule 18 (Financial Distress) only, all references to “Key Sub-contractor” shall not include telecommunications carriers used by the Supplier in the provision of Services except for any telecommunications company that is an Affiliate of the Supplier. As at the Effective Date such telecommunications carriers that are excluded from the definition of Key Sub-contractor in this Schedule are Openreach Limited and Virgin Media Wholesale Limited:

2 WARRANTIES AND DUTY TO NOTIFY

- 2.1 The Supplier warrants and represents to the Authority for the benefit of the Authority that as at the Effective Date:
- (a) the long-term credit ratings issued for each entity in the FDE Group by each of the Rating Agencies are as set out in Annex 2 of this Schedule; and
 - (b) the financial position or, as appropriate, the financial performance of each of the Supplier and Key Sub-contractors satisfies:
 - (i) the Financial Target Thresholds; and
 - (ii) the financial target thresholds and mitigation measures set out in the FVRA updated prior to the Effective Date.
- 2.2 The Supplier shall promptly notify (or shall procure that its auditors promptly notify) the Authority in writing if there is any downgrade in the credit rating issued by any Rating Agency for any entity in the FDE Group (and in any event within 5 Working Days of the occurrence of the downgrade).
- 2.3 The Supplier shall:
- (a) regularly monitor the credit ratings of each entity in the FDE Group with the Rating Agencies;
 - (b) review and submit to the Authority an updated FVRA once a year within one hundred and twenty (120) days after the Accounting Reference Date;
 - (c) monitor and report on the Financial Indicators for each entity in the FDE Group against the Financial Target Thresholds at least at the frequency set out for each at Paragraph 5.1 (where specified) and in any event, on a regular basis and no less than once a year within one hundred and twenty (120) days after the Accounting Reference Date; and
 - (d) promptly notify (or shall procure that its auditors promptly notify) the Authority in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event (and in any event, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

the fact, circumstance or matter which could cause a Financial Distress Event).

- 2.4 For the purposes of determining whether a Financial Distress Event has occurred pursuant to the provisions of Paragraphs 3.1(a), and for the purposes of determining relief under Paragraph 7.1, the credit rating of an FDE Group entity shall be deemed to have dropped below the applicable Credit Rating Threshold if:
- (a) any of the Rating Agencies have given a Credit Rating Level for that entity which is below the applicable Credit Rating Threshold; or
 - (b) a Rating Agency that is specified as holding a Credit Rating for an entity as set out at Annex 2 of this Schedule ceases to hold a Credit Rating for that entity.
- 2.5 Each report submitted by the Supplier pursuant to Paragraph 2.3(b) shall:
- (a) be a single report with separate sections for each of the FDE Group entities;
 - (b) contain a sufficient level of information to enable the Authority to verify the calculations that have been made in respect of the Financial Indicators;
 - (c) include key financial and other supporting information (including any accounts data that has been relied on) as separate annexes;
 - (d) be based on the audited accounts for the date or period on which the Financial Indicator is based or, where the Financial Indicator is not linked to an accounting period or an accounting reference date, on unaudited management accounts prepared in accordance with their normal timetable; and
 - (e) include a history of the Financial Indicators reported by the Supplier in graph form to enable the Authority to easily analyse and assess the trends in financial performance.

3 FINANCIAL DISTRESS EVENTS

- 3.1 The following shall be Financial Distress Events:
- (a) the credit rating of an FDE Group entity dropping below the applicable Credit Rating Threshold;
 - (b) an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;
 - (c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity;

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (d) an FDE Group entity committing a material breach of covenant to its lenders;
- (e) a Key Sub-contractor notifying the Authority that the Supplier has not satisfied any material sums properly due under a specified invoice and not subject to a genuine dispute;
- (f) any FDE Group entity extends the filing period for filing its accounts with the Registrar of Companies so that the filing period ends more than 9 months after its accounting reference date without an explanation to the Authority which the Authority (acting reasonably) considers to be adequate;
- (g) any FDE Group entity is late to file its annual accounts without a public notification or an explanation to the Authority which the Authority, acting reasonably, considers to be adequate;
- (h) the directors and/or external auditors of any FDE Group entity conclude that a material uncertainty exists in relation to that FDE Group entity's going concern in the annual report including in a reasonable but plausible downside scenario. This includes, but is not limited to, commentary about liquidity and trading prospects in the reports from directors or external auditors;
- (i) any of the following:
 - (i) any FDE Group entity makes a public announcement which contains adverse commentary with regards to that FDE Group entity's liquidity and trading and trading prospects, such as but not limited to, a profit warning or ability to trade as a going concern;
 - (ii) commencement of any litigation against an FDE Group entity with respect to financial indebtedness greater than £5m or obligations under a service contract with a total contract value greater than £5m;
 - (iii) non-payment by an FDE Group entity of any financial indebtedness;
 - (iv) any financial indebtedness of an FDE Group entity becoming due as a result of an event of default;
 - (v) the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity; or
 - (vi) the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity;

in each case which the Authority reasonably believes (or would be likely reasonably to believe) could directly impact on the continued

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

performance and delivery of the Services in accordance with this Contract;

- (j) following the annual submission of the FVRA, the Authority failing to be satisfied (acting in line with prevailing Guidance) with any mitigation proposed by the Supplier in response to one or more of the metrics in the FVRA; and
- (k) any one of the Financial Indicators set out at Paragraph 5 for any of the FDE Group entities failing to meet the required Financial Target Threshold, except where the Authority is satisfied (acting in line with prevailing Guidance) with any mitigation for the relevant Financial Indicator proposed by the Supplier.

4 CONSEQUENCES OF FINANCIAL DISTRESS EVENTS

- 4.1 Immediately upon notification by the Supplier of a Financial Distress Event (or if the Authority becomes aware of a Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and the Authority shall have the rights and remedies as set out in Paragraphs 4.3 to 4.5.
- 4.2 In the event of a late or non-payment of a Key Sub-contractor pursuant to Paragraph 3.1(e), the Authority shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier 10 Working Days to:
 - (a) rectify such late or non-payment; or
 - (b) demonstrate to the Authority's reasonable satisfaction that there is a valid reason for late or non-payment.
- 4.3 The Supplier shall (and shall procure that any Monitored Supplier and/or any relevant Key Sub-contractor shall):
 - (a) at the request of the Authority, meet the Authority as soon as reasonably practicable (and in any event within 3 Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Authority may permit and notify to the Supplier in writing) to review the effect of the Financial Distress Event on the continued performance and delivery of the Services in accordance with this Contract; and
 - (b) where the Authority reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3(a)) that the Financial Distress Event could impact on the continued performance and delivery of the Services in accordance with this Contract:
 - (i) submit to the Authority for its approval, a draft Financial Distress Remediation Plan as soon as reasonably practicable (and in any event, within 10 Working Days of the initial notification (or awareness) of the Financial Distress

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Event or such other period as the Authority may permit and notify to the Supplier in writing); and

- (ii) to the extent that it is legally permitted to do so and subject to Paragraph 4.7, provide such information relating to the Supplier, any Monitored Supplier and/or Key Sub-contractors as the Authority may reasonably require in order to understand the risk to the Services, which may include forecasts in relation to cash flow, orders and profits and details of financial measures being considered to mitigate the impact of the Financial Distress Event.

4.4 The Authority shall not withhold its approval of a draft Financial Distress Remediation Plan unreasonably. If the Authority does not approve the draft Financial Distress Remediation Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Remediation Plan, which shall be resubmitted to the Authority within 5 Working Days of the rejection of the first draft. This process shall be repeated until the Financial Distress Remediation Plan is either:

- (a) approved by the Authority;
- (b) referred, by notice sent by either Party to the other Party explaining why it thinks the Financial Distress Remediation Plan has not been approved, to commercial negotiation led by senior representatives who have authority to agree the Financial Distress Remediation Plan to be held within 28 days of the date of the notice; or
- (c) finally rejected by the Authority.

4.5 Following approval of the Financial Distress Remediation Plan by the Authority, the Supplier shall:

- (a) on a regular basis (which shall not be less than fortnightly):
 - (i) review and make any updates to the Financial Distress Remediation Plan as the Supplier may deem reasonably necessary and/or as may be reasonably requested by the Authority, so that the plan remains adequate, up to date and ensures the continued performance and delivery of the Services in accordance with this Contract; and
 - (ii) provide a written report to the Authority setting out its progress against the Financial Distress Remediation Plan, the reasons for any changes made to the Financial Distress Remediation Plan by the Supplier and/or the reasons why the Supplier may have decided not to make any changes;
- (b) where updates are made to the Financial Distress Remediation Plan in accordance with Paragraph 4.5(a), submit an updated Financial Distress Remediation Plan to the Authority for its

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

approval, and the provisions of Paragraphs 4.4 and 4.5(a) shall apply to the review and approval process for the updated Financial Distress Remediation Plan; and

- (c) comply with the Financial Distress Remediation Plan (including any updated Financial Distress Remediation Plan) and ensure that it achieves the financial and performance requirements set out in the Financial Distress Remediation Plan.
- 4.6 Where the Supplier reasonably believes that the relevant Financial Distress Event under Paragraph 4.1 (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify the Authority and the Parties may agree that the Supplier shall be relieved of its obligations under Paragraph 4.5.
- 4.7 The Supplier shall use reasonable endeavours to put in place the necessary measures to ensure that the information specified at Paragraph 4.3(b)(ii) is available when required and on request from the Authority and within reasonable timescales. Such measures may include:
- (a) obtaining in advance written authority from Key Sub-contractors and/or Monitored Suppliers authorising the disclosure of the information to the Authority and/or entering into confidentiality agreements which permit disclosure;
 - (b) agreeing in advance with the Authority, Key Sub-contractors and/or Monitored Suppliers a form of confidentiality agreement to be entered by the relevant parties to enable the disclosure of the information to the Authority;
 - (c) putting in place any other reasonable arrangements to enable the information to be lawfully disclosed to the Authority (which may include making price sensitive information available to Authority nominated personnel through confidential arrangements, subject to their consent); and
 - (d) disclosing the information to the fullest extent that it is lawfully entitled to do so, including through the use of redaction, anonymisation and any other techniques to permit disclosure of the information without breaching a duty of confidentiality.

5 FINANCIAL INDICATORS

- 5.1 Subject to the calculation methodology set out at Annex 3 of this Schedule, the Financial Indicators and the corresponding calculations and thresholds used to determine whether a Financial Distress Event has occurred in respect of those Financial Indicators, shall be as follows:

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Financial Indicator	Calculation¹	Financial Target Threshold:	Monitoring and Reporting Frequency
1 - Turnover Ratio	<i>Turnover Ratio = Bidder Annual Revenue / Expected Annual Contract Value</i>	<i>> 6.00 times</i>	<i>Tested and reported yearly in arrears within 120 days of each accounting reference date based upon figures for the 12 months ending on the relevant accounting reference date.</i>
2 - Operating Margin	<i>Operating Margin = Operating Profit / Revenue</i>	<i>> 10.00%</i>	<i>Tested and reported yearly in arrears within 120 days of each accounting reference date based upon figures for the 12 months ending on the relevant accounting reference date.</i>
3 - Net Debt to EBITDA Ratio	<i>Net Debt to EBITDA ratio = Net Debt / EBITDA</i>	<i>< 3.00 times</i>	<i>Tested and reported yearly in arrears within 120 days of each accounting reference date based upon EBITDA for the 12 months ending on, and Net Debt at, the relevant accounting reference date.</i>
4 - Net Debt + Net Pension Deficit to EBITDA ratio	<i>Net Debt + Net Pension Deficit to EBITDA Ratio = (Net Debt + Net Pension Deficit) / EBITDA</i>	<i>< 4.50 times</i>	<i>Tested and reported yearly in arrears within 120 days of each accounting reference date based upon EBITDA for the 12 months ending on, and the Net Debt and Net Pension Deficit at, the relevant accounting reference date</i>

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Financial Indicator	Calculation¹	Financial Target Threshold:	Monitoring and Reporting Frequency
5 - Net Interest Paid Cover	<i>Net Interest Paid Cover = Earnings Before Interest and Tax / Net Interest Paid</i>	<i>> 4.50 times</i>	<i>Tested and reported yearly in arrears within 120 days of each accounting reference date based upon figures for the 12 months ending on the relevant accounting reference date.</i>
6 - Acid Ratio	<i>Acid Ratio = (Current Assets – Inventories) / Current Liabilities</i>	<i>> 0.80 times</i>	<i>Tested and reported yearly in arrears within 120 days of each accounting reference date based upon figures at the relevant accounting reference date.</i>
7 - Net Asset value	<i>Net Asset Value = Net Assets</i>	<i>> NIL</i>	<i>Tested and reported yearly in arrears within 120 days of each accounting reference date based upon figures at the relevant accounting reference date.</i>
8 - Group Exposure Ratio	<i>Group Exposure / Gross Assets</i>	<i>< 30.00%</i>	<i>Tested and reported yearly in arrears within 120 days of each accounting reference date based upon figures at the relevant accounting reference date.</i>

Key: ¹ – See Annex 3 of this Schedule which sets out the calculation methodology to be used in the calculation of each Financial Indicator.

5.2 Monitored Suppliers

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Monitored Supplier	Applicable Financial Indicators (these are the Financial Indicators from the table in Paragraph 5.1 which are to apply to the Monitored Suppliers)
N/A	1 Turnover Ratio 2 Operating Margin 3 Net Debt to EBITDA Ratio 4 Net Debt + Net Pension Deficit to EBITDA ratio 5 Net Interest Paid Cover 6 Acid Ratio 7 Net Asset value 8 Group Exposure Ratio
N/A	1 Turnover Ratio 2 Operating Margin 3 Net Debt to EBITDA Ratio 4 Net Debt + Net Pension Deficit to EBITDA ratio 5 Net Interest Paid Cover 6 Acid Ratio 7 Net Asset value 8 Group Exposure Ratio

6 TERMINATION RIGHTS

- 6.1 The Authority shall be entitled to terminate this Contract under Clause 31.1(b) (*Termination by the Authority*) if:
- (a) the Supplier fails to notify the Authority of a Financial Distress Event in accordance with Paragraph 2.3(d);
 - (b) the Supplier fails to comply with any part of Paragraph 4.3;

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (c) the Authority finally rejects a Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraphs 4.4 to 4.5(a); and/or
- (d) the Supplier fails to comply with the terms of the Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraph 4.5(c).

7 PRIMACY OF CREDIT RATINGS

7.1 Without prejudice to the Supplier's obligations and the Authority's rights and remedies under Paragraph 2, if, following the occurrence of a Financial Distress Event pursuant to any of Paragraphs 3.1(b) to 3.1(j), the Rating Agencies review and report subsequently that the credit ratings for the FDE Group entities do not drop below the relevant Credit Rating Thresholds specified for those entities in Annex 2 of this Schedule, then:

- (a) the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.5; and
- (b) the Authority shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3(b)(ii).

8 BOARD CONFIRMATION

8.1 If this Contract has been specified as a Critical Service Contract under Paragraph 1.1 of Part B to Schedule 26 (*Service Continuity Plan and Corporate Resolution Planning*) then, subject to Paragraph 8.4 of this Schedule, the Supplier shall within one hundred and twenty (120) days after each Accounting Reference Date or within 15 months of the previous Board Confirmation (whichever is the earlier) provide a Board Confirmation to the Authority in the form set out at Annex 4 of this Schedule, confirming that to the best of the Board's knowledge and belief, it is not aware of and has no knowledge:

- (a) that a Financial Distress Event has occurred since the later of the Effective Date or the previous Board Confirmation or is subsisting; or
- (b) of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event.

8.2 The Supplier shall ensure that in its preparation of the Board Confirmation it exercises due care and diligence and has made reasonable enquiry of all relevant Supplier Personnel and other persons as is reasonably necessary to understand and confirm the position.

8.3 In respect of the first Board Confirmation to be provided under this Contract, the Supplier shall provide the Board Confirmation within 15 months of the Effective Date if earlier than the timescale for submission set out in Paragraph 8.1 of this Schedule.

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 8.4 Where the Supplier is unable to provide a Board Confirmation in accordance with Paragraphs 8.1 to 8.3 of this Schedule due to the occurrence of a Financial Distress Event or knowledge of subsisting matters which could reasonably be expected to cause a Financial Distress Event, it will be sufficient for the Supplier to submit in place of the Board Confirmation, a statement from the Board of Directors to the Authority (and where the Supplier is a Strategic Supplier, the Supplier shall send a copy of the statement to the Cabinet Office Markets and Suppliers Team) setting out full details of any Financial Distress Events that have occurred and/or the matters which could reasonably be expected to cause a Financial Distress Event.

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 1: RATING AGENCIES AND THEIR STANDARD RATING SYSTEM

- **Standard and Poors**

- Credit Rating Level 1 = AAA
- Credit Rating Level 2 = AA+
- Credit Rating Level 3 = AA
- Credit Rating Level 4 = AA-
- Credit Rating Level 5 = A+
- Credit Rating Level 6 = A
- Credit Rating Level 7 = A-
- Credit Rating Level 8 = BBB+
- Credit Rating Level 9 = BBB
- Credit Rating Level 10 = BBB-
- Credit Rating Level 11 = BB+
- Credit Rating Level 12 = BB
- Credit Rating Level 13 = BB-
- Credit Rating Level 14 = B+
- Credit Rating Level 15 = B
- Credit Rating Level 16 = B-
- Credit Rating Level 17 = CCC+
- Credit Rating Level 18 = CCC
- Credit Rating Level 19 = CCC-
- Credit Rating Level 20 = CC
- Credit Rating Level 21 = C
- Credit Rating Level 22 = RD
- Credit Rating Level 23 = SD
- Credit Rating Level 24 = D

- **Company Watch H-Score**

- 1 to 100

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 2: CREDIT RATINGS AND CREDIT RATING THRESHOLDS

Entity	Credit Rating (long term) (insert credit rating issued for the entity at the Effective Date)	Credit Rating Threshold (insert the actual rating (e.g. AA-) or the Credit Rating Level (e.g. Credit Rating Level 3))
Supplier		

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 3: CALCULATION METHODOLOGY FOR FINANCIAL INDICATORS

The Supplier shall ensure that it uses the following general and specific methodologies for calculating the Financial Indicators against the Financial Target Thresholds:

General methodology

- 1 *Terminology:* The terms referred to in this Annex are those used by UK companies in their financial statements. Where the entity is not a UK company, the corresponding items should be used even if the terminology is slightly different (for example a charity would refer to a surplus or deficit rather than a profit or loss).
- 2 *Groups:* Where the entity is the holding company of a group and prepares consolidated financial statements, the consolidated figures should be used.
- 3 *Foreign currency conversion:* Figures denominated in foreign currencies should be converted at the exchange rate in force at the relevant date for which the Financial Indicator is being calculated.
- 4 *Treatment of non-underlying items:* Financial Indicators should be based on the figures in the financial statements before adjusting for non-underlying items.

Specific Methodology

Financial Indicator	Specific Methodology
1 Turnover Ratio	Revenue should be shown on the face of the Income Statement in a standard set of financial statements. It should exclude the entity's share of the revenue of joint ventures or associates.
2 Operating Margin	The elements used to calculate the Operating Margin should be shown on the face of the Income Statement in a standard set of financial statements. Figures for Operating Profit and Revenue should exclude the entity's share of the results of any joint ventures or Associates. Where an entity has an operating loss (i.e. where the operating profit is negative), Operating Profit should be taken to be zero.
3 Net Debt to EBITDA Ratio	<i>"Net Debt" = Bank overdrafts + Loans and borrowings + Finance leases + Deferred consideration payable – Cash and cash equivalents</i>

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Financial Indicator	Specific Methodology
	<i>“EBITDA” = Operating profit + Depreciation charge + Amortisation charge</i> The majority of the elements used to calculate the Net Debt to EBITDA Ratio should be shown on the face of the Balance sheet, Income statement and Statement of Cash Flows in a standard set of financial statements but will otherwise be found in the notes to the financial statements. <i>Net Debt:</i> The elements of Net Debt may be described slightly differently and should be found either on the face of the Balance Sheet or in the relevant note to the financial statements. All interest bearing liabilities (other than retirement benefit obligations) should be included as borrowings as should, where disclosed, any liabilities (less any assets) in respect of any hedges designated as linked to borrowings (but not non-designated hedges). Borrowings should also include balances owed to other group members. Deferred consideration payable should be included in Net Debt despite typically being non-interest bearing. Cash and cash equivalents should include short-term financial investments shown in current assets. Where Net debt is negative (i.e. an entity has net cash), the relevant Financial Target Threshold should be treated as having been met. <i>EBITDA:</i> Operating profit should be shown on the face of the Income Statement and, for the purposes of calculating this Financial Indicator, should include the entity’s share of the results of any joint ventures or Associates. <i>The depreciation and amortisation charges for the period may be found on the face of the Statement of Cash Flows or in a Note to the Accounts. Where EBITDA is negative, the relevant Financial Target Threshold should be treated as not having been met (unless Net Debt is also negative, in which case the relevant Financial Target Threshold should be treated as having been met).]</i>
4 Net Debt + Net Pension Deficit to EBITDA ratio	<i>“Net Debt” = Bank overdrafts + Loans and borrowings + Finance leases + Deferred consideration payable – Cash and cash equivalents</i> <i>“Net Pension Deficit” = Retirement Benefit Obligations – Retirement Benefit Assets</i>

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Financial Indicator	Specific Methodology
	<i>“EBITDA” = Operating profit + Depreciation charge + Amortisation charge</i> The majority of the elements used to calculate the Net Debt + Net Pension Deficit to EBITDA Ratio should be shown on the face of the Balance sheet, Income statement and Statement of Cash Flows in a standard set of financial statements but will otherwise be found in the notes to the financial statements. <u>Net Debt:</u> The elements of Net Debt may be described slightly differently and should be found either on the face of the Balance Sheet or in the relevant note to the financial statements. All interest bearing liabilities (other than retirement benefit obligations) should be included as borrowings as should, where disclosed, any liabilities (less any assets) in respect of any hedges designated as linked to borrowings (but <i>not</i> non-designated hedges). Borrowings should also include balances owed to other group members. Deferred consideration payable should be included in Net Debt despite typically being non-interest bearing. Cash and cash equivalents should include short-term financial investments shown in current assets. <u>Net Pension Deficit:</u> Retirement Benefit Obligations and Retirement Benefit Assets may be shown on the face of the Balance Sheet or in the notes to the financial statements. They may also be described as pension benefits / obligations, post-employment obligations or other similar terms. Where ‘Net Debt + Net Pension Deficit’ is negative, the relevant Financial Target Threshold should be treated as having been met. <u>EBITDA:</u> Operating profit should be shown on the face of the Income Statement and, for the purposes of calculating this Financial Indicator, should include the entity’s share of the results of any joint ventures or Associates. The depreciation and amortisation charges for the period may be found on the face of the Statement of Cash Flows or in a Note to the Accounts. Where EBITDA is negative, the relevant Financial Target Threshold should be treated as not having been met

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Financial Indicator	Specific Methodology
	(unless 'Net Debt + Net Pension Deficit' is also negative, in which case the relevant Financial Target Threshold should be regarded as having been met).
5 Net Interest Paid Cover	<i>"Earnings Before Interest and Tax" = Operating profit</i> <i>"Net Interest Paid" = Interest paid – Interest received</i> Operating profit should be shown on the face of the Income Statement in a standard set of financial statements and, for the purposes of calculating this Financial Indicator, should include the entity's share of the results of any joint ventures or Associates. Interest received and interest paid should be shown on the face of the Cash Flow statement. Where Net interest paid is negative (i.e. the entity has net interest received), the relevant Financial Target Threshold should be treated as having been met.
6 Acid Ratio	All elements that are used to calculate the Acid Ratio are available on the face of the Balance Sheet in a standard set of financial statements.
7 Net Asset value	Net Assets are shown (but sometimes not labelled) on the face of the Balance Sheet of a standard set of financial statements. Net Assets are sometimes called net worth or 'Shareholders' Funds'. They represent the net assets available to the shareholders. Where an entity has a majority interest in another entity in which there are also minority or non-controlling interests (i.e. where it has a subsidiary partially owned by outside investors), Net Assets should be taken inclusive of minority or non-controlling interests (as if the entity owned 100% of such entity).
8 Group Exposure Ratio	<i>"Group Exposure" = Balances owed by Group Undertakings + Contingent liabilities assumed in support of Group Undertakings</i> <i>"Gross Assets" = Fixed Assets + Current Assets</i> <u>Group Exposure</u>: Balances owed by (i.e. receivable from) Group Undertakings are shown within Fixed assets or Current assets either on the face of the Balance Sheet or in the relevant notes to the financial statements. In many cases there may be no such balances, in particular where

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Financial Indicator	Specific Methodology
	an entity is not a member of a group or is itself the ultimate holding company of the group. Contingent liabilities assumed in support of Group Undertakings are shown in the Contingent Liabilities note in a standard set of financial statements. They include guarantees and security given in support of the borrowings of other group companies, often as part of group borrowing arrangements. Where the contingent liabilities are capped, the capped figure should be taken as their value. Where no cap or maximum is specified, the relevant Financial Target Threshold should automatically be regarded as not having been met. In many cases an entity may not have assumed any contingent liabilities in support of Group Undertakings, in particular where an entity is not a member of a group or is itself the ultimate holding company of the group. <u>Gross Assets</u>: Both Fixed assets and Current assets are shown on the face of the Balance Sheet

SCHEDULE 18 (FINANCIAL DISTRESS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 4: BOARD CONFIRMATION

Supplier Name:

Contract Reference Number:

The Board of Directors acknowledge the requirements set out at paragraph 8 of **Schedule 18 (*Financial Distress*)** and confirm that the Supplier has exercised due care and diligence and made reasonable enquiry of all relevant Supplier Personnel and other persons as is reasonably necessary to enable the Board to prepare this statement.

The Board of Directors confirms, to the best of its knowledge and belief, that as at the date of this Board Confirmation it is not aware of and has no knowledge:

- (a) that a Financial Distress Event has occurred since the later of the previous Board Confirmation and the Effective Date or is subsisting;
or
- (b) of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event

On behalf of the Board of Directors:

Chair	
Signed	
Date	
Director	
Signed	
Date	

SCHEDULE 19 (FINANCIAL REPORTS AND AUDIT RIGHTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 19

FINANCIAL REPORTS AND AUDIT RIGHTS

SCHEDULE 19 (FINANCIAL REPORTS AND AUDIT RIGHTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 19 (*Financial Reports and Audit Rights*)

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

“Annual Contract Report”	the annual contract report to be provided by the Supplier to the Authority pursuant to Paragraph 1 of Part B;
“Audit Agents”	(a) the Authority’s internal and external auditors; (b) the Authority’s statutory or regulatory auditors; (c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; (d) HM Treasury or the Cabinet Office; (e) any party formally appointed by the Authority to carry out audit or similar review functions; and (f) successors or assigns of any of the above;
“Contract Amendment Report”	the contract amendment report to be provided by the Supplier to the Authority pursuant to Paragraph 1 of Part B;
“Final Reconciliation Report”	the final reconciliation report to be provided by the Supplier to the Authority pursuant to Paragraph 1 of Part B;
“Financial Model”	the Contract Inception Report, the latest Annual Contract Report or the latest Contract Amendment Report, whichever has been most recently approved by the Authority in accordance with Paragraph 2 of Part B;
“Financial Reports”	the Contract Inception Report and the reports listed in the table in Paragraph 1.1 of Part B;
“Financial Representative”	a reasonably skilled and experienced member of the Supplier’s staff who has specific responsibility for preparing, maintaining, facilitating access to,

SCHEDULE 19 (FINANCIAL REPORTS AND AUDIT RIGHTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

discussing and explaining the Open Book Data and Financial Reports;

“Financial Transparency Objectives”

has the meaning given in Paragraph 1 of Part A;

“Material Change”

a Change which:

- (a) materially changes the profile of the Charges; or
- (a) varies the total Charges payable during the Term (as forecast in the latest Financial Model) by:
 - (i) 5% or more; or
 - (ii) £1m or more;

“Onerous Contract”

a contract in which the unavoidable costs of meeting the obligations under the contract exceed the economic benefits expected to be received under it, as defined under International Accounting Standard 37;

“Onerous Contract Report”

means a report provided by the Supplier pursuant to Paragraph 3 of Part A to this Schedule;

“Open Book Data”

complete and accurate financial and non-financial information which is sufficient to enable the Authority to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the Term, including details and all assumptions relating to:

- (a) the Supplier's Costs broken down against each Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all hardware and software;
- (b) operating expenditure relating to the provision of the Services including an analysis showing:
 - (i) the unit costs and quantity of consumables and bought-in services;

SCHEDULE 19 (FINANCIAL REPORTS AND AUDIT RIGHTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- (ii) manpower resources broken down into the number and grade/role of all Supplier Personnel (free of any contingency) together with a list of agreed rates against each manpower grade;
 - (iii) a list of Costs underpinning those rates for each manpower grade, being the agreed rate less the Supplier's Profit Margin; and
 - (iv) Reimbursable Expenses;
- (c) Overheads;
- (d) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Services;
- (e) the Supplier Profit achieved over the Term and on an annual basis;
- (f) confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods applied generally by the Supplier;
- (g) an explanation of the type and value of risk and contingencies associated with the provision of the Services, including the amount of money attributed to each risk and/or contingency; and
- (h) the actual Costs profile for each Service Period.

SCHEDULE 19 (FINANCIAL REPORTS AND AUDIT RIGHTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

PART A: FINANCIAL TRANSPARENCY OBJECTIVES AND OPEN BOOK DATA**1 FINANCIAL TRANSPARENCY OBJECTIVES**

1.1 The Supplier acknowledges that the provisions of this Schedule are designed (inter alia) to facilitate, and the Supplier shall co-operate with the Authority in order to achieve, the following objectives:

(a) **Understanding the Charges**

- (i) for the Authority to understand any payment sought from it by the Supplier including an analysis of the Costs, Overhead recoveries (where relevant), time spent by Supplier Personnel in providing the Services and the Supplier Profit Margin;
- (ii) for both Parties to be able to understand the Financial Model and Cost forecasts and to have confidence that these are based on justifiable numbers and appropriate forecasting techniques;
- (iii) to facilitate the use of Guaranteed Maximum Price with Target Cost pricing mechanisms (where relevant as referred to in Schedule 15 (*Charges and Invoicing*));

(b) **Agreeing the impact of Change**

- (i) for both Parties to agree the quantitative impact of any Changes that affect ongoing costs and to identify how these could be mitigated and/or reflected in the Supplier's Charges;
- (ii) for both Parties to be able to review, address issues with and re-forecast progress in relation to the provision of the Services;

(c) **Continuous improvement**

- (i) for the Parties to challenge each other with ideas for efficiency and improvements; and
- (ii) to enable the Authority to demonstrate that it is achieving value for money for the tax payer relative to current market prices,

(together the "**Financial Transparency Objectives**").

2 OPEN BOOK DATA

2.1 The Supplier acknowledges the importance to the Authority of the Financial Transparency Objectives and the Authority's need for complete transparency in the way in which the Charges are calculated.

2.2 During the Term, and for a period of 7 years following the end of the Term, the Supplier shall:

SCHEDULE 19 (FINANCIAL REPORTS AND AUDIT RIGHTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- (a) maintain and retain the Open Book Data; and
- (b) disclose and allow the Authority and/or the Audit Agents access to the Open Book Data.

3 ONEROUS CONTRACTS

- 3.1 If the Supplier publicly designates the Contract as an Onerous Contract (including where the Supplier has identified the Contract as such in any published accounts or public reports and announcements), the Supplier shall promptly notify the Authority of the designation and shall then prepare and deliver to the Authority within the timescales agreed by the Parties (and in any event, no later than 2 months following the publication of the designation) a draft Onerous Contract Report which includes the following:
- (a) An initial root cause analysis of the issues and circumstances which may have contributed to the Contract being designated as an Onerous Contract;
 - (b) An initial risk analysis and impact assessment on the provision of the Services as a result of the Supplier's designation of the Contract as an Onerous Contract;
 - (c) the measures which the Supplier intends to put in place to minimise and mitigate any adverse impact on the provision on the Services;
 - (d) details of any other options which could be put in place to remove the designation of the Contract as an Onerous Contract and/or which could minimise and mitigate any adverse impact on the provision of the Services.
- 3.2 Following receipt of the Onerous Contract Report, the Authority shall review and comment on the report as soon as reasonably practicable and the Parties shall cooperate in good faith to agree the final form of the report, which shall be submitted to the Commercial Board, such final form report to be agreed no later than 1 month following the Authority's receipt of the draft Onerous Contract Report.
- 3.3 The Commercial Board shall meet within 14 Working Days of the final Onerous Contract Report being agreed by the Parties to discuss the contents of the report; and the Parties shall procure the attendance at the meeting of any key participants where reasonably required (including the Cabinet Office Markets and Suppliers team where the Supplier is a Strategic Supplier; representatives from any Key Sub-contractors/Monitored Suppliers; and the project's senior responsible officers (or equivalent) for each Party).
- 3.4 The Supplier acknowledges and agrees that the report is submitted to the Authority and the Commercial Board on an information only basis and the Authority and the Commercial Board's receipt of and comments in relation to the report shall not be deemed to be an acceptance or rejection of the report nor shall it relieve the Supplier of any liability under this Contract. Any

SCHEDULE 19 (FINANCIAL REPORTS AND AUDIT RIGHTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Changes to be agreed by the Parties pursuant to the report shall be subject to the Change Control Procedure.

SCHEDULE 19 (FINANCIAL REPORTS AND AUDIT RIGHTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

PART B: FINANCIAL REPORTS**1 PROVISION OF THE FINANCIAL REPORTS**

1.1 The Supplier shall provide

- (a) the Contract Inception Report on or before the Effective Date; and
- (b) during the Term the following financial reports to the Authority, in the frequency specified below:

Financial Report	When to be provided
Contract Amendment Report	Within 1 month of a Material Change being agreed between the Supplier and the Authority
Quarterly Contract Report	Within 1 month of the end of each Quarter
Annual Contract Report	Within 1 month of the end of the Contract Year to which that report relates
Final Reconciliation Report	Within 6 months after the end of the Term
Payment Planner	Monthly in accordance with Schedule 15 (Charges and Invoicing)

1.2 The Supplier shall provide to the Authority the Financial Reports in the same software package (Microsoft Excel or Microsoft Word), layout and format as the blank templates which have been issued by the Authority to the Supplier on or before the Effective Date for the purposes of this Contract. The Authority shall be entitled to modify the template for any Financial Report by giving written notice to the Supplier, including a copy of the updated template.

1.3 A copy of each Financial Report shall be held by both the Authority and the Supplier. If there is a Dispute regarding a Financial Report, the Authority's copy of the relevant Financial Report shall be authoritative.

1.4 Each Financial Report shall:

- (a) be completed by the Supplier using reasonable skill and care;
- (b) incorporate and use the same defined terms as are used in this Contract;
- (c) quote all monetary values in pounds sterling;

SCHEDULE 19 (FINANCIAL REPORTS AND AUDIT RIGHTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- (d) quote all Costs as exclusive of any VAT; and
 - (e) quote all Costs and Charges based on current prices.
- 1.5 Each Annual Contract Report and the Final Reconciliation Report shall be certified by the Supplier's Chief Financial Officer or Director of Finance (or equivalent as agreed in writing by the Authority in advance of issue of the relevant Financial Report), acting with express authority, as:
- (a) being accurate and not misleading;
 - (b) having been prepared in conformity with generally accepted accounting principles within the United Kingdom;
 - (c) being a true and fair reflection of the information included within the Supplier's management and statutory accounts; and
 - (d) compliant with the requirements of Paragraph 1.6.
- 1.6 The Supplier shall:
- (a) prepare each Financial Report using the same methodology as that used for the Contract Inception Report;
 - (b) to the extent permitted by Law, ensure that each Annual Contract Report and each Contract Amendment Report (if any) is a true and fair reflection of the Costs and Supplier Profit Margin forecast by the Supplier;
 - (c) to the extent permitted by Law, ensure that the Final Reconciliation Report is a true and fair reflection of the Costs; and
 - (d) not have any other internal financial model in relation to the Services inconsistent with the Financial Model.
- 1.7 During the Term, and for a period of 18 months following the end of the Term, the Supplier shall make available the Financial Representative at reasonable times and on reasonable notice to answer any queries that the Authority may have on any of the Financial Reports and/or Open Book Data.
- 1.8 If the Supplier becomes aware of the occurrence, or the likelihood of the future occurrence, of an event which will or may have a material effect on the following:
- (a) the Costs incurred (or those forecast to be incurred) by the Supplier; and/or
 - (b) the forecast Charges for the remainder of the Term,
- the Supplier shall, as soon as practicable, notify the Authority in writing of the event in question detailing the actual or anticipated effect. For the avoidance of doubt, notifications provided in accordance with this Paragraph 1.8 shall not have the effect of amending any provisions of this Contract.

SCHEDULE 19 (FINANCIAL REPORTS AND AUDIT RIGHTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

2 FINANCIAL MODEL

2.1 Following the delivery by the Supplier of each Annual Contract Report and any Contract Amendment Report:

- (a) the Parties shall meet to discuss its contents within 10 Working Days of receipt (or such other period as the Parties shall agree). The Financial Representative shall attend the meeting;
- (b) the Supplier shall make appropriate Supplier Personnel and advisers available to discuss any variations between the relevant Financial Report and the Contract Inception Report or immediately preceding Annual Contract Report or Contract Amendment Report (as the case may be) and to explain such variations (with reference to supporting evidence) to the satisfaction of the Authority; and
- (c) the Authority shall either within 10 Working Days of the meeting referred to in Paragraph 2.1(a) notify the Supplier that:
 - (i) the relevant Financial Report contains errors or omissions or that further explanations or supporting information is required, in which event the Supplier shall make any necessary modifications to the Financial Report and/or supply the Authority with such supporting evidence as is required to address the Authority's concerns within 10 Working Days of such notification and the Authority shall following receipt of such amended Financial Report and/or supporting information, approve or reject such Financial Report; or
 - (ii) the Authority has approved the relevant Financial Report.

2.2 Following approval by the Authority of the relevant Financial Report in accordance with Paragraph 2.1(c), that version shall become, with effect from the date of such approval, the current approved version of the Financial Model for the purposes of this Contract, a version of which shall be held by both the Authority and the Supplier. If there is a Dispute regarding a Financial Report, the Authority's copy of the relevant Financial Report shall be authoritative.

2.3 If the Parties are unable to reach agreement on any Financial Report within 30 Working Days of its receipt by the Authority, the matter shall be referred for determination in accordance with Schedule 23 (*Dispute Resolution Procedure*).

3 DISCUSSION OF QUARTERLY CONTRACT REPORTS AND FINAL RECONCILIATION REPORT

3.1 Following the delivery by the Supplier of each Quarterly Contract Report, the Parties shall meet to discuss its contents within 10 Working Days of receipt (or such other period as the Parties shall agree). The Financial Representative shall attend the meeting.

SCHEDULE 19 (FINANCIAL REPORTS AND AUDIT RIGHTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- 3.2 Following the delivery by the Supplier of the Final Reconciliation Report, the Parties shall meet to discuss its contents within 10 Working Days of receipt (or such other period as the Parties shall agree). The Financial Representative shall attend the meeting.

4 KEY SUB CONTRACTORS

- 4.1 The Supplier shall, if requested by the Authority, provide (or procure the provision of) a report or reports including the level of information set out in the Financial Reports in relation to the costs and expenses to be incurred by any of its Key Sub-contractors.

- 4.2 Without prejudice to Paragraph 1.1 of Part C, the Supplier shall:

- (a) be responsible for auditing the financial models/reports of its Key Sub-contractors and for any associated costs and expenses incurred or forecast to be incurred; and
- (b) on written request by the Authority, provide the Authority or procure that the Authority is provided with:
 - (i) full copies of audit reports for the Key Sub-contractors. The Authority shall be entitled to rely on such audit reports; and
 - (ii) further explanation of, and supporting information in relation to, any audit reports provided.

SCHEDULE 19 (FINANCIAL REPORTS AND AUDIT RIGHTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

PART C: AUDIT RIGHTS**1 AUDIT RIGHTS**

- 1.1 The Authority, acting by itself or through its Audit Agents, shall have the right during the Term and for a period of 18 months thereafter, to assess compliance by the Supplier and/or its Key Sub-contractors of the Supplier's obligations under this Contract, including for the following purposes:
- (a) to verify the integrity and content of any Financial Report;
 - (b) to verify the accuracy of the Charges and any other amounts payable by the Authority under this Contract (and proposed or actual variations to such Charges and payments);
 - (c) to verify the Costs (including the amounts paid to all Sub-contractors and any third party suppliers);
 - (d) to verify the Certificate of Costs and/or the Open Book Data;
 - (e) to verify the Supplier's and each Key Sub-contractor's compliance with this Contract and applicable Law;
 - (f) to identify or investigate actual or suspected fraud, impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations;
 - (g) to identify or investigate any circumstances which may impact upon the financial stability of the Supplier and/or any Key Sub-contractors or their ability to perform the Services;
 - (h) to obtain such information as is necessary to fulfil the Authority's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General;
 - (i) to review any books of account and the internal contract management accounts kept by the Supplier in connection with this Contract;
 - (j) to carry out the Authority's internal and statutory audits and to prepare, examine and/or certify the Authority's annual and interim reports and accounts;
 - (k) to enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority has used its resources;
 - (l) to verify the accuracy and completeness of any Management Information delivered or required by this Contract;

SCHEDULE 19 (FINANCIAL REPORTS AND AUDIT RIGHTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- (m) to review any Performance Monitoring Reports and/or other records relating to the Supplier's performance of the Services and to verify that these reflect the Supplier's own internal reports and records;
 - (n) to inspect the IT Environment (or any part of it) and the wider service delivery environment (or any part of it);
 - (o) to review the accuracy and completeness of the Registers;
 - (p) to review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;
 - (q) to review the Supplier's quality management systems (including all relevant Quality Plans and any quality manuals and procedures);
 - (r) to review the Supplier's compliance with the Standards;
 - (s) to inspect the Authority Assets, including the Authority's IPRs, equipment and facilities, for the purposes of ensuring that the Authority Assets are secure and that any register of assets is up to date; and/or
 - (t) to review the integrity, confidentiality and security of the Authority Data.
- 1.2 Except where an audit is imposed on the Authority by a regulatory body or where the Authority has reasonable grounds for believing that the Supplier has not complied with its obligations under this Contract, the Authority may not conduct an audit of the Supplier or of the same Key Sub-contractor more than twice in any Contract Year.
- 1.3 Nothing in this Contract shall prevent or restrict the rights of the Comptroller and/or Auditor General and/or their representatives from carrying out an audit, examination or investigation of the Supplier and/or any of the Key Sub-contractors for the purposes of and pursuant to applicable Law.
- 2 CONDUCT OF AUDITS**
- 2.1 The Authority shall during each audit comply with those security, sites, systems and facilities operating procedures of the Supplier that the Authority deems reasonable and use its reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Supplier or delay the provision of the Services.
- 2.2 Subject to the Authority's obligations of confidentiality, the Supplier shall on demand provide the Authority and the Audit Agents with all reasonable co-operation and assistance (and shall procure such co-operation and assistance from its Sub-contractors) in relation to each audit, including:
- (a) all information requested by the Authority within the permitted scope of the audit;

SCHEDULE 19 (FINANCIAL REPORTS AND AUDIT RIGHTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- (b) reasonable access to any Sites and to any equipment used (whether exclusively or non-exclusively) in the performance of the Services;
 - (c) access to the Supplier System; and
 - (d) access to Supplier Personnel.
- 2.3 The Supplier shall implement all measurement and monitoring tools and procedures necessary to measure and report on the Supplier's performance of the Services against the applicable Performance Indicators at a level of detail sufficient to verify compliance with the Performance Indicators.
- 2.4 The Authority shall endeavour to (but is not obliged to) provide at least 15 Working Days' notice of its intention to conduct an audit.
- 2.5 The Parties agree that they shall bear their own respective costs and expenses incurred in respect of compliance with their obligations under this Paragraph 2, unless the audit identifies a material Default by the Supplier in which case the Supplier shall reimburse the Authority for all the Authority's reasonable costs incurred in connection with the audit.
- 3 USE OF SUPPLIER'S INTERNAL AUDIT TEAM**
 - 3.1 As an alternative to the Authority's right pursuant to Paragraph 1.1 to exercise an audit either itself or through its Audit Agents, the Authority may require in writing that an audit is undertaken by the Supplier's own internal audit function for any of the purposes set out in Paragraph 1.1.
 - 3.2 Following the receipt of a request from the Authority under Paragraph 3.1 above, the Supplier shall procure that the relevant audit is undertaken as soon as reasonably practicable and that the Authority has unfettered access to:
 - (a) the resultant audit reports; and
 - (b) all relevant members of the Supplier's internal audit team for the purpose of understanding such audit reports.
- 4 RESPONSE TO AUDITS**
 - 4.1 If an audit undertaken pursuant to Paragraphs 1 or 3 identifies that:
 - (a) the Supplier has committed a Default, the Authority may (without prejudice to any rights and remedies the Authority may have) require the Supplier to correct such Default as soon as reasonably practicable and, if such Default constitutes a Notifiable Default, to comply with the Rectification Plan Process;
 - (b) there is an error in a Financial Report, the Supplier shall promptly rectify the error;
 - (c) the Authority has overpaid any Charges, the Supplier shall pay to the Authority:

SCHEDULE 19 (FINANCIAL REPORTS AND AUDIT RIGHTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- (i) the amount overpaid;
 - (ii) interest on the amount overpaid at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from the date of overpayment by the Authority up to the date of repayment by the Supplier; and
 - (iii) the reasonable costs incurred by the Authority in undertaking the audit,
- the Authority may exercise its right to deduct such amount from the Charges if it prefers; and
- (d) the Authority has underpaid any Charges, the Supplier shall not be entitled to increase the Charges paid or payable by the Authority.

SCHEDULE 20 (ANTICIPATED SAVINGS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 20

ANTICIPATED SAVINGS

SCHEDULE 20 (ANTICIPATED SAVINGS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 20 (*Anticipated Savings*)

[Drafting Note – No indicative savings are defined for the Effective Date. However, this schedule is retained in the instance that it is required post Effective Date.]

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SCHEDULE 21

GOVERNANCE

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Schedule 21 (*Governance*)

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

“Board Member” the initial persons appointed by the Authority and the Supplier to the Boards as set out in Annex 1 and any replacements from time to time agreed by the Parties in accordance with Paragraph 6.3;

“Board” any of the boards described in Annex 2;

2 INTRODUCTION

2.1 This Schedule describes the elements and layers of the governance structure and each Party’s roles and responsibilities within that governance structure.

2.2 The governance framework set out in Figure 1 illustrates the governance Boards which will be used to manage and govern this Contract.

2.3 The Parties recognise that their relationship needs to be managed in relation to this Contract but also in the context of:

2.3.1 the Other Suppliers; and

2.3.2 facilitating the smooth and flexible exit of the Services to one or more Replacement Suppliers during the Term.

2.4 This Schedule (including the governance framework in Figure 1) shall be reviewed annually in accordance with Paragraph 8 (Annual Review) and amended if it is agreed by the Parties that amendments are necessary in order to enable the Parties’ intent described in Paragraphs 2.2, 2.3 and 3.1 to continue to be met effectively. Any amendments agreed by the Parties under this Paragraph 2.4 shall be implemented in accordance with the Change Control Procedure.

2.5 Nothing in this Schedule regarding joint activity by the Parties shall be taken to lessen or remove the obligations on the Supplier as set out in this Contract.

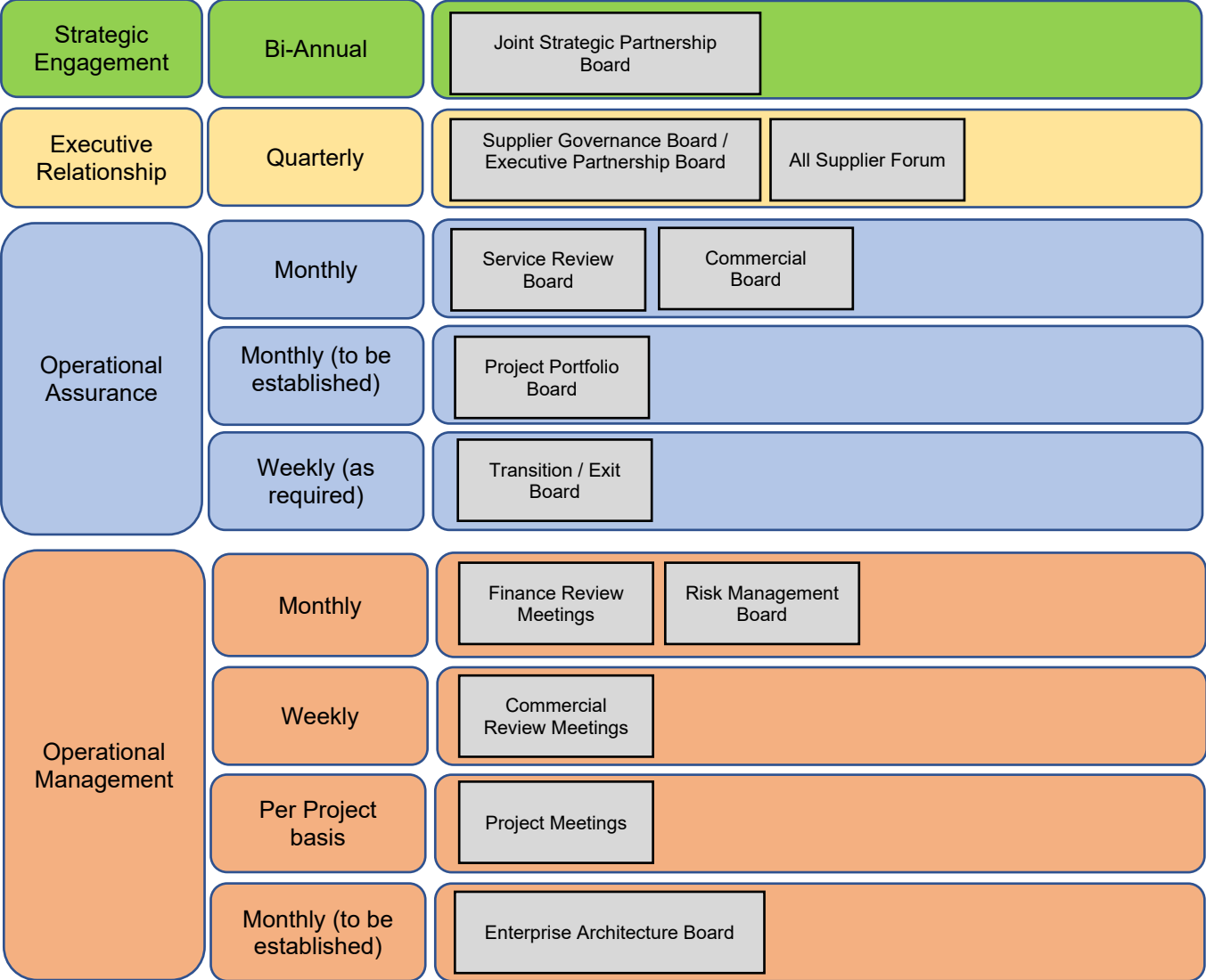
SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

3 GOVERNANCE FRAMEWORK

3.1 The Parties shall comply with the provisions in this Schedule and in particular shall establish the governance framework described in Figure 1 and



Paragraph 6 below in accordance with the general principles and provisions

Figure 1 – Governance Framework

4 MANAGEMENT OF THE SERVICES

- 4.1 The Supplier and the Authority shall each appoint a manager for the purposes of this Contract through whom the provision of the Services shall be managed day-to-day.
- 4.2 The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 4.3 The Parties agree to operate the Boards specified in Annex 2 to this Schedule.

5 ENGAGEMENT LEVELS

- 5.1 The governance framework outlined in Figure 1 defines the service management and assurance mechanisms, contract management, communication channels and working relationships between the Parties at four (4) engagement levels.

Strategic Engagement Level

- 5.2 This level brings together senior executives from the Authority and the Supplier to provide direction on activities that lead to increased understanding of mutual objectives, ensuring alignment with the Authority's strategic digital and technology objectives and influence behavioural changes to drive improvements to the quality and health of the relationship.

Executive Relationship Level

- 5.3 This level brings together executives and senior managers from the Authority and the Supplier to review the quality of the relationship from a service delivery, commercial, project and technical perspective.
- 5.4 The Executive Relationship Level also serves as an escalation forum to resolve issues which have not been resolved at the Operational Assurance Level.

Operational Assurance Level

- 5.5 This level brings together senior managers from the Authority and the Supplier to manage, monitor and review deliverables, service and outcomes, including, but not limited to, the relevant approval criteria and Performance Indicators.
- 5.6 The Operational Assurance level also serves as an escalation forum to resolve issues which have not been resolved at the Operational Management level.

Operational Management Level

- 5.7 This level brings together operational and commercial personnel from the Authority and the Supplier to discuss and review operational performance data and contract and commercial variations.
- 5.8 The Operational Management level will also include a series of tactical meetings supporting each of the Operational Assurance Level Boards. Examples of these meetings would include project meetings and commercial review meetings.

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Key Sub-Contractors

- 5.9 To the extent that the Supplier requires the support and input of its Key Sub-contractor(s) at any of the Boards, the Supplier shall procure that its Key Sub-contractor(s) attend such Boards as may be required.
- 5.10 The Authority acknowledges and agrees that in certain circumstances it will be appropriate and/or necessary for the Supplier Personnel, including personnel of any Key Sub-contractor(s), to attend the Boards, provided always that the Supplier shall remain responsible for all acts and omissions of its Key Sub-contractor(s) and the acts and omissions of those employed or engaged by the Key Sub-contractor(s) as if they were its own.
- 5.11 The Supplier shall not be entitled to any increase in the Charges for any input or support provided by any Key Sub-contractor to any of the Boards in accordance with provisions of Paragraphs 5.9 and 5.10.

6 BOARDS**Establishment and structure of the Boards**

- 6.1 The Boards shall be established by the Authority for the purposes of this Contract on which both the Supplier and the Authority shall be represented.
- 6.2 In relation to each Board, the:
- (a) responsibilities and functions;
 - (b) Authority Board Members;
 - (c) Supplier Board Members;
 - (d) frequency that the Board shall meet (unless otherwise agreed between the Parties);
 - (e) location of the Board's meetings; and
 - (f) planned start date by which the Board shall be established,
- shall be as set out in Annex 2.
- 6.3 In the event that either Party wishes to replace any of its appointed Board Members as set out in the relevant terms of reference, that Party shall notify the other in writing of the proposed change for agreement by the other Party (such agreement not to be unreasonably withheld or delayed). Notwithstanding the foregoing, it is intended that each Authority Board Member has at all times a counterpart Supplier Board Member of equivalent seniority and expertise.

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Board meetings

- 6.4 Each Party shall ensure that its Board Members shall make all reasonable efforts to attend Board meetings at which that Board Member's attendance is required.
- 6.4B Board Members may be substituted where the Board's terms of reference allow for such substitution and where the relevant Party has delegated appropriate authority to the substitute member.
- 6.4C If any Board Member is not able to attend a Board meeting, that person shall use all reasonable endeavours to ensure that:
- (a) a delegate attends the relevant Board meeting in his/her place who (wherever possible) is properly briefed and prepared; and
 - (b) that he/she is debriefed by such delegate after the Board meeting.
- 6.5 A chairperson shall be appointed by the Authority for each Board as identified in Annex 2 (whether from the Supplier Personnel or the Authority staff). The chairperson shall be responsible for:
- (a) scheduling Board meetings;
 - (b) setting the agenda for Board meetings and circulating to all attendees in advance of such meeting;
 - (c) chairing the Board meetings;
 - (d) monitoring the progress of any follow up tasks and activities agreed to be carried out following Board meetings;
 - (e) ensuring that minutes for Board meetings are recorded and disseminated electronically to the appropriate persons and to all Board meeting participants within seven Working Days after the Board meeting; and
 - (f) facilitating the process or procedure by which any decision agreed at any Board meeting is given effect in the appropriate manner.
- 6.6 Board meetings shall be quorate as long as at least two representatives from each Party are present.
- 6.7 The Parties shall ensure, as far as reasonably practicable, that all Boards shall as soon as reasonably practicable resolve the issues and achieve the objectives placed before them. Each Party shall endeavour to ensure that Board Members are empowered to make relevant decisions or have access to empowered individuals for decisions to be made to achieve this.

7 CONTRACT MANAGEMENT MECHANISMS

- 7.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Contract.

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

7.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Authority, processes for:

- (a) the identification and management of risks;
- (b) the identification and management of issues; and
- (c) monitoring and controlling project plans.

7.3 The Risk Register shall be updated by the Supplier and submitted for review by both Parties at the relevant Board meetings.

8 ANNUAL REVIEW

8.1 An annual review meeting shall be held throughout the Term on a date to be agreed between the Parties, either combined with a meeting of the Joint Strategic Partnership Board or in addition to the Boards outlined in this Schedule (at the discretion of the Authority Representative).

8.2 The annual review meeting shall be attended by the Supplier Representative and the Authority Representative and any other persons considered by the Authority necessary for the review.

8.3 The agenda for the annual review meeting shall be agreed between the Parties and shall include (without limitation):

8.3.1 the Supplier's performance of the Services in accordance with this Contract;

8.3.2 options for improving relationships and working practices between the Parties and with Other Suppliers including, if necessary, changes to the governance framework;

8.3.3 proposed ways of improving the achievement of Performance Indicators and Target Performance Levels, value for money, or the effectiveness of the Services in supporting the Authority's business; and

8.3.4 any other matters as communicated in writing by the Authority.

9 INFORMAL MEETINGS

9.1 This Schedule shall not prejudice the ability of the Parties to arrange informal meetings to discuss specific issues and ongoing project and service requirements relating to this Contract as necessary. The Parties shall cooperate to find the convenient times and locations for such meetings and use reasonable endeavours to ensure that all identified attendees attend such meetings.

9.2 A list of informal meetings currently planned will be agreed between the Parties within ten (10) Working Days of the Effective Date.

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 1 - GOVERNANCE PRINCIPLES**1. GENERAL**

- 1.1 The Authority will develop the governance framework to refine and add more detail, based on the provisions in this Schedule, and the Supplier shall agree to the amended and refined governance framework under the Change Control Procedure. Provided that the resource requirements imposed on the Supplier by such further developed governance framework do not increase materially, the Supplier shall not be entitled to recover any additional costs from the Authority in relation to it.
- 1.2 The governance framework will establish a single, centralised structure to deal with all issues that relate to the performance and commercial aspects of this Contract or in-flight programmes of work.
- 1.3 This Schedule defines the governance structures that the Parties will establish to ensure that:
 - (a) appropriate forums exist to manage this Contract;
 - (b) appropriate information is maintained and shared to enable the Authority to oversee and ensure the delivery of the Services;
 - (c) Documentation is provided to timescales and the requisite quality and, where appropriate, are maintained and updated; and
 - (d) the effectiveness of the Services, the Parties' relationship and the governance framework are reviewed regularly and improved where appropriate.

2. PRINCIPLES

- 2.1 The Parties recognise that relationships will exist at many levels between them, and this Schedule reflects these relationships within a formal process covering the decision-making, communication channels and escalation paths that the Parties shall use.
- 2.2 The Parties shall, through the proper application of these principles, procedures and structures, ensure that strong, healthy, responsive and mutually beneficial collaborative relationships are built and maintained between the Parties at all levels.
- 2.3 The Suppliers will take their direction from the Authority in all their dealings under this Contract, and not from any other government department or agency.
- 2.4 The Parties shall ensure that they, through collaborative participation in the Boards, as soon as reasonably practicable resolve all issues arising in relation to the Services and this Contract and achieve all agreed objectives for each of the Boards. Each Party shall use reasonable endeavours to ensure that members of the Board are empowered to make relevant decisions or have access to empowered individuals for decisions to be made.

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 2.5 All Parties shall agree and implement processes to regularly measure the health and effectiveness of the relationship and work together to agree and implement desirable improvements to the governance framework.
- 2.6 The membership and frequency of the Boards will be sufficient to manage and assure the end-to-end delivery of quality and cost-effective Services by the Supplier to the Authority, including:
- a) delivery of the Operational Services in accordance with Clause 7 (Performance Indicators); and
 - b) delivery of the Transitional Services in accordance with Paragraph 7 (TS Performance Levels) of Schedule 34.
- 2.7 Each Board will work across all Services other than where specified in the governance framework and the provisions of this Schedule.
- 2.8 All governance interactions (including work approval, new services, business requirements, etc) between the Supplier, Other Suppliers, Replacement Suppliers and the Authority will be managed in line with the governance framework.
- 2.9 The Boards will determine, authorise and prioritise Changes in Services and otherwise fully support the Authority's changing business objectives and requirements.
- 2.10 The Boards will include Authority and Supplier representation as appropriate, and may include Sub-contractors and Other Suppliers engaged by the Authority if required and agreed by the Authority.
- 2.11 The Supplier is expected to actively participate with the relevant Other Suppliers, except where issues of commercial confidentiality arise and have (where practicable) been agreed in advance with the Authority.
- 2.12 Without limiting the Supplier's general obligations to provide advance warning (where practicable), the Supplier shall take such steps as are necessary to ensure that no material issues are raised in Board meetings without giving the Authority prior notice.

3. OBJECTIVES

- 3.1 This Schedule sets out the governance structures for managing and assuring the Services to be delivered by the Supplier to the Authority and will include:
- (a) the communication and governance from and between the Authority and the Supplier;
 - (b) the Boards and associated roles and responsibilities;
 - (c) the overall portfolio management and governance organisation to manage and assure the Services;
 - (d) the architectural governance forums to assure delivery and operational conformance to prescribed standards;
 - (e) information assurance governance;

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (f) the service management and governance forums to manage and assure the Services through the service delivery lifecycle;
 - (g) the programme management and governance forums to manage, deliver and assure the Services; and
 - (h) the Supplier management and governance forums to manage, monitor and assure the commercial aspects relating to the provision and support of the Services.
- 3.2 The Supplier shall support and enable the Authority to monitor and manage the Services and other obligations and shall provide all reasonable co-operation to the Authority with the objective of ensuring that the performance of the Services and its other obligations, shall be achieved in an efficient and cost effective manner in accordance with the terms of this Contract.
- 3.3 As and when necessary, the Authority will define and agree with the Supplier the terms of reference for each of the Boards and forums defined in the governance framework. The terms of reference for each Board and forum will include:
 - (a) Frequency;
 - (b) Type;
 - (c) Chair;
 - (d) Input;
 - (e) Participants;
 - (f) Roles and Responsibilities/Escalation;
 - (g) Value/Purpose;
 - (h) Input Reports; and
 - (i) Expected Outcomes.
- 3.4 The Supplier shall support the Authority through the provision of:
 - (a) core membership (standing attendees);
 - (b) optional attendees (as required or requested);
 - (c) responsibilities, accountabilities and limits of decision-making ability including, but not limited to, financial, business impact and business risk;
 - (d) inputs; and
 - (e) outputs.
- 3.5 The Supplier shall support the Authority by providing, on the request of the Authority, current organisational information, including:

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (a) Supplier governance and guidance organisation: includes as a minimum, organisation charts, description of functions performed, and contact information;
 - (b) Supplier management and delivery organisations: includes (where agreed with the Authority), organisation charts, description of functions performed, and contact information;
 - (c) key contacts - Supplier: The list of Supplier contacts (with contact information), who are key managers of the Services and/or who perform a liaison function in regard to the Services including, but not limited to, business unit and geographic region; and
 - (d) key governance documentation: Reference material relating to governance forums e.g. operational meeting minutes, performance reports etc.
- 3.6 The Authority will act as the facilitator for all Boards and will ensure the following:
- (a) clear communications and directives relating to outcomes of all governance and change forums;
 - (b) that all concerned parties are actively involved in changes that will or may have an impact on the Services being delivered;
 - (c) the Authority will relay any risks identified across the Supplier and Other Suppliers; and
 - (d) the Authority will provide a secretariat function, including:
 - i. scheduling Board meetings;
 - ii. ensuring all Board agendas and papers are circulated to the members of the respective Board in accordance with the timescales set out in this schedule, unless an extraordinary meeting has been scheduled or an urgent item has been added to the agenda and it is not possible to meet this requirement, in which case as much notice as is practicable shall be given;
 - iii. ensuring that minutes for Board meetings are recorded and disseminated electronically to the appropriate persons and to all Board meeting participants within three (3) Working Days following the Board meeting;
 - iv. monitoring the progress of any follow up tasks and activities agreed to be carried out following Board meetings; and
 - v. facilitating the process or procedure by which any decision agreed at any Board meeting is given effect in the appropriate manner.

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 3.7 The Supplier acknowledges that the Authority shall act as the facilitator for all Boards and that the Authority shall provide services to the Supplier (as described in Paragraph (d) The Supplier shall support the Authority in delivering the services as described in paragraph (d) through, including:
- (a) attendance at scheduled Board meetings by an appropriately empowered representative;
 - (b) monitoring and progressing any follow up tasks and activities agreed to be carried out before or following Board meetings; and
 - (c) facilitating the process or procedure by which any decision agreed at any Board meeting is given effect in the appropriate manner.

4. GOVERNANCE STRUCTURE, BOARDS AND FORUMS

- 4.1 Each Board or forum will be responsible for resolving any operational disagreements or other issues regarding the provision of the Services, the Performance Indicators and performance under any additional work that may be awarded under this Contract and, if required, to support the issue resolution mechanisms and Dispute Resolution Procedure.
- 4.2 The effectiveness of the governance framework will be evaluated from time to time by the Authority and the Supplier to identify improvements or efficiencies and modified accordingly.
- 4.3 The Authority reserves the right, acting reasonably, to convene a meeting with any or all parties at any time and will provide as sufficient notice as is practicable.
- 4.4 Time and resource cost of participation in the Boards and development of their policies, processes and procedures shall be borne by the party incurring it.
- 4.5 The chairperson shall be responsible for:
- (a) setting the agenda for Board meetings (based on suggestions from the Authority and/or the Suppliers); and
 - (b) chairing the Board meetings.
- 4.6 The chairperson of each Board will record decisions and agreements reached at the Board, based on the discussions and the input/feedback received from all participants. Each Board meeting will be outcome based and defined outcomes will be delivered and realised within the agreed timescales. The decisions of the Board shall be binding on both Parties.
- 4.7 The Supplier shall supply appropriately senior, authorised, qualified and experienced personnel to the Boards as required.

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 2 - REPRESENTATION AND STRUCTURE OF BOARDS

Joint Strategic Partnership Board – Steering Level

Responsibilities and Functions of the Joint Strategic Partnership Board	Forum for annual review as described in Paragraph 8 of Schedule 21, unless the annual review is held separately. Act as forward-looking forum to enable the Authority to deliver its vision and to review challenges (e.g. spending constraints) and the Supplier’s position on such challenges. Ensure the strategic alignment of the Authority and Supplier businesses. Inform the Supplier of any relevant changes to the Authority’s business and services strategy. Having sight of all the IT deliverables for programmes and Projects residing on the Authority portfolio. Review the overall performance of both the Supplier and the Authority. Track delivery against the jointly agreed initiatives and improvement opportunities to maximise value from the relationship. Review the overall effectiveness of the Services in meeting the needs of the Authority’s business. Review the relationship status between the Parties. Facilitate the exchange of future directional information. Making key resource deployment and investment priority decisions. Inform the Authority of any updates to any relevant Supplier global technology initiatives.

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	Once every 12 months, the Supplier will report on services improvements as required under Clause 8.1. Resolve relationship issues and issues relating to this Contract which are escalated to the Joint Strategic Partnership Board. Review of risks appropriate to this board to be included as a standing agenda item. Share output of risk review with cascading Boards/forums.
Authority Members of Joint Strategic Partnership Board	[REDACTED] Authority Representative [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Supplier Members of Joint Strategic Partnership Board	[REDACTED] Supplier Representative [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Start Date for Joint Strategic Partnership Board meetings	Post Effective Date to align with the Authority governance framework
Frequency of Joint Strategic Partnership Board meetings	Annually, or bi-annually if requested by either Party

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Location of Joint Strategic Partnership Board meetings	Authority headquarters or 10 South Colonnade

Supplier Governance Board – Executive Level

Responsibilities and Functions of the Supplier Governance Board	Review the relationship between the Authority and the Supplier. Monitor the alignment of the Authority and Supplier objectives. Provide direction on activities to drive improvements to the health and quality of the relationship via the Supplier Performance Review Board. Track delivery against the jointly agreed initiatives following the value assessment which identifies opportunities from the Supplier Performance Review Board to maximise value from the relationship. Review the Supplier scorecard to understand how the Supplier is performing against its key metrics. Review of risks appropriate to this board to be included as a standing agenda item. Share output of risk review with cascading Boards/forums. Serve as an executive escalation forum to resolve non-urgent issues which have not been resolved at the Boards below it. Establish and communicate delivery priorities. Carry out activities in relation to audit reviews carried out in accordance with this Contract as appropriate.
Authority Members of Supplier Governance Board	Authority Representative (Chairperson) [REDACTED]

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	[REDACTED] [REDACTED] [REDACTED] [REDACTED]
Supplier Members of Supplier Governance Board	Supplier Representative [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Start Date for Supplier Governance Board meetings	Within 3 months of Transitional Services Commencement Date
Frequency of Supplier Governance Board meetings	Quarterly
Location of Supplier Governance Board meetings	Authority Headquarters or 10 South Colonnade or Supplier site

All Supplier Forum – Executive Level

Responsibilities and Functions of the All Supplier Forum	To align the Parties and Other Suppliers for delivery of End to End Services. To provide a forum for the Authority to provide key messages to the Supplier and Other Suppliers. To identify technical and operational innovations which may bring wider benefit to the Authority’s technology estate. To share innovation and best practices.

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	Note that this forum's function relates to relationship management rather than contract management.
Authority Members of All Supplier Forum	[REDACTED] [REDACTED] [REDACTED] [REDACTED]
Supplier Members of All Supplier Forum	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Start Date for All Supplier Forum	Post Effective Date to align with the Authority governance framework
Frequency of All Supplier Forum	Quarterly
Location of All Supplier Forum	Authority Headquarters or 10 South Colonnade

Transition / Exit Board – Operational Assurance Level

Responsibilities and Functions of the Transition / Exit Board	This Board may be constituted as a Transition Board, an Exit Board, or a Transition and Exit Board, depending on Transition / Exit activities at the time. Transition-related functions and responsibilities: • Review progress of the Implementation Plan and Transition matters. • Oversight of Transition Framework as applicable to the Implementation Services, including status of 'gates' of the Transition Framework.

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	• Oversight / management of Product Descriptions, Documentary Deliverables and other artefacts required to support the Implementation Plan • Review of Transition-related risks, issues, assumptions and dependencies Exit-related functions and responsibilities: • Develop strategy for exit of Services • Manage and review the Exit Plan. • Oversee the implementation of the Exit Plan and any Termination Assistance Services until the conclusion of all activities set out in the Exit Plan and/or Termination Assistance Plan. • Oversight / management of Registers and other documents required to support the Exit Plan • Review of Exit-related risks, issues, assumptions and dependencies
Authority Members for Transition / Exit Board	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Supplier Members for Transition / Exit Board	[REDACTED]

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Start Date for Transition / Exit Board meetings	Promptly following the Effective Date
Frequency of Transition / Exit Board meetings	During Transition or Exit of Services: weekly unless otherwise agreed Otherwise: Either Party's [REDACTED] may require the Exit Board to convene if required to progress / review the Exit Plan and/or compliance with Schedule 25 (up to once during any quarter)
Location of Transition / Exit Board meetings	Authority Headquarters or 10 South Colonnade and/or online

Service Review Board – Operational Assurance Level

Responsibilities and Functions of the Service Review Board	Monitor compliance by the Supplier with the Processes and the Authority's policies and procedures. Act as an escalation point for the sub-groups governing lower-level activities in the Operating Environment. Resolve all escalations brought and escalate only under exceptional circumstances. Receive and review reports from, and act as escalation body for, the Transition / Exit Board and/or the Exit. Formal escalation from the Transition / Exit Board. Review of open risks appropriate to this board to be included as a standing

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	agenda item. Share output of risk review with cascading Boards/forums. Service Performance: a) Review the Supplier's performance against Performance Levels and TS Service Levels; b) Review all Service Points incurred and Service Credits due; c) Review the Supplier's performance against the end-to-end measures that reflect the ITIL processes; d) Review the Supplier's performance against the strategic Authority business measures; and e) Review any draft Rectification Plans submitted by the Supplier. Review and approval of any operational Changes Review the status of operational assets Review any Security Incidents raised and mitigating actions Financial Performance: a) Review the financial data submitted by the Supplier, Supplier Relationship: a) Review any survey results for relationship maturity and effectiveness; b) Review any service improvement plans and/or rectification plans; and

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	c) Review any matters pertaining to activities with Other Suppliers (whether in respect of the Services or of the Other Suppliers' services provided to the Authority). Review of all open risks appropriate to this board to be included as a standing agenda item. Share output of risk review with cascading Boards/forums
Authority Members for Service Performance Review Board	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Supplier Members for Service Performance Review Board	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Start Date for Service Performance Review Board meetings	Post Effective Date to align with the Authority governance framework
Frequency of Service Performance Review Board meetings	Monthly or as required by the Authority from time to time.
Location of Service Performance Review Board meetings	Authority Headquarters or 10 South Colonnade

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Commercial Board – Operational Assurance Level

Responsibilities and Functions of the Commercial Board	Monitor in relation to this Contract the overall commercial relationship. Monitor the alignment of the Authority and Supplier commercial objectives. Take a pro-active view of commercial impacts, stakeholder management and communication issues. Monitor, discuss and resolve contract compliance and commercial issues escalated to the Commercial Board. Resolve wherever possible all major Supplier and Authority commercial performance issues and Disputes relating to this Contract as are referred to it. Ensure implementation of best practice in contract and compliance management. Provide a forum for achieving a collective and consistent view of compliance against all Contract obligations. Deal with and make decisions on issues identified by the Supplier or the Authority that require contract or compliance management action, resolution Contract. Review of all open risks appropriate to this board to be included as a standing agenda item. Share output of risk review with cascading Boards/forums. Monitor the agreed working at risk register. Review the Authority commercial risk register (quarterly basis).

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	Review the continuity of supply in the Supplier's supply chain process. Agree actions and improvement plans to address compliance issues. Appoint, as and when required, "contract management teams" with responsibility for seeking resolution of contractual disputes. Review issues in purchase order processing and Service Request and items where there are delays or other issues in progress. Maintain an overview of contract Change. Discuss diversity and equality issues.
Authority Members for Commercial Board	[REDACTED] [REDACTED] [REDACTED]
Supplier Members for Commercial Board	[REDACTED] [REDACTED] [REDACTED]
Start Date for Commercial Board meetings	Milestone 1b (Transitional Services Commencement)
Frequency of Commercial Board meetings	Monthly or as required by the Authority from time to time.
Location of Commercial Board meetings	Authority Headquarters or 10 South Colonnade

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Project Portfolio Board – Operational Assurance Level

Responsibilities and Functions of the Project Portfolio Board	Evaluate major change programmes and the associated feasibility studies and business cases to support these changes. Manage agreed business transformation programmes. Provide high level direction, prioritisation, against other current and planned activities, integration, and co-ordination across all projects. Monitor the development and implementation of current and future Projects. Monitor the status of Projects during the lifecycle of Changes. Identify, monitor and manage risks in the delivery of Projects or the Services. Monitor the impact of any risks associated with any major changes to the Authority’s IT systems, architecture and/or network, including in relation to Projects and new services in so far as such IT systems relate to the Services. Review of all open risks appropriate to this board to be included as a standing agenda item. Share output of risk review with cascading Boards/forums.
Authority Members for Project Portfolio Board	Authority Representative (Chairperson) [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Supplier Members for Project Portfolio Board	Supplier Representative [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Start Date for Project Portfolio Board meetings	<i>Following Achievement of Milestone M1b (Transitional Services mobilisation complete)</i>
Frequency of Project Portfolio Board meetings	Monthly unless otherwise agreed.
Location of Project Portfolio Board meetings	Authority Headquarters or 10 South Colonnade

Risk Management Board – Operational Management Level

Responsibilities and Functions of the Risk Management Board	To identify, review and agree management of risks and issues. Ensure all elements of new/open risks (description, cause, effect, controls, mitigation, actions, scores, and target dates) are captured and reviewed. Review of all open risks appropriate to this board to be included as a standing agenda item (including security management and data processing risks). On Quarterly basis, amended agenda to include a detailed review of key risks. Share output of risk review with cascading Boards/forums.

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	Note: Supplier to circulate risk treatment plan 5 days in advance of each meeting.
Authority Members for Risk Management Board	[REDACTED] Authority Representative [REDACTED] [REDACTED] [REDACTED] Authority Representative [REDACTED]
Supplier Members for Risk Management Board	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Start Date for Risk Management Board	Following Achievement of Milestone M1b (Transitional Services mobilisation complete)
Frequency of Risk Management Board	Monthly or as required by the Authority from time to time.
Location of Risk Management Board	Authority Headquarters or 10 South Colonnade

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Finance Review Meetings – Operational Management Level

Responsibilities and Functions of the Finance Review Meetings	Review of the current financial status of the Contract and identify any actions as required. Review the financial reports submitted by the Supplier.
Authority Members for Finance Review Meetings	[REDACTED] [REDACTED] [REDACTED] Authority Representative [REDACTED] [REDACTED] [REDACTED]
Supplier Members for Finance Review Meetings	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Start Date for Finance Review Meetings	Following Achievement of Milestone M1b (Transitional Services mobilisation complete)
Frequency of Finance Review Meetings	Monthly or as required by the Authority from time to time.
Location of Finance Review Meetings	Authority Headquarters or 10 South Colonnade

Project Meetings – Per Project Basis

Responsibilities and Functions of the Project Meetings	Discuss any address any open risks and that may impact the delivery of Services.

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	Agree any required improvement plans and/or rectification plans relating to Services. Monitor the Supplier performance against any agreed Service Improvement Plans.
Authority Members for Project Meetings	[REDACTED] [REDACTED]
Supplier Members for Project Meetings	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Start Date for Project Meetings	Following Achievement of Milestone M1b (Transitional Services mobilisation complete)
Frequency of Project Meetings	Monthly and as otherwise decided on a per project basis.
Location of Project Meetings	Authority Headquarters or 10 South Colonnade

Commercial Review Meetings – Operational Management Level

Responsibilities and Functions of the Commercial Review Meetings	Identify, review, and resolve any commercial issues raised from within Project Meetings and Financial Review Meetings.

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	Resolve any Contract compliance and commercial issues. Ensure alignment of the Parties commercial objectives/ obligations Escalate and report to the Commercial Board as required.
Authority Members for Commercial Review Meetings	[REDACTED] Authority Representative [REDACTED]
Supplier Members for Commercial Review Meetings	[REDACTED] [REDACTED] [REDACTED]
Start Date for Commercial Review Meetings	Following Achievement of Milestone M1b (Transitional Services mobilisation complete)
Frequency of Commercial Review Meetings	Weekly or as required by the Authority from time to time.
Location of Commercial Review Meetings	Authority Headquarters or 10 South Colonnade

Enterprise Architecture Board – Operational Management Level

Responsibilities and Functions of the Enterprise Architecture Board	This Board shall be a joint Authority and Supplier forum chaired by the Authority with additional representatives from IT and the supplier community to provide insight to the supplier community on Authority strategic direction, and to enable a collaborative approach to the development of enterprise IT architecture and innovation. It will: Coordinate the interface between the various suppliers.

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	Provide the main forum for the Authority to share corporate and business unit strategic aims with suppliers. Provide a forum for the Authority to issue innovation challenges to suppliers, with a view to encouraging collaborative working between suppliers in a pre-commercial mode. Provide a forum to explain Authority strategic architectural direction on capabilities, products and services. Formally communicate any changes in the Authority Enterprise Architecture Services to suppliers. Provide a mechanism for suppliers to challenge the Authority Enterprise Architecture Services, and propose new directions, approaches and insight to maintain the Enterprise Architecture Services flexibility. Provide a mechanism to enable joint horizon scanning to identify business and technology trends the Authority should assess. Monitor the status of Projects during the lifecycle of Changes. Ensure that the Authority's IT systems, infrastructure and network are appropriately secure in accordance with Schedule 5 (Security Management). Review of all open risks appropriate to this board to be included as a standing agenda item. Share output of risk review with cascading Boards/forums.
Authority Members for Enterprise Architecture Board	[REDACTED] [REDACTED]
Supplier Members for Enterprise Architecture Board	[REDACTED]

SCHEDULE 21 (GOVERNANCE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Start Date for Enterprise Architecture Board meetings	Following Achievement of Milestone M1b (Transitional Services mobilisation complete)
Frequency of Enterprise Architecture Board meetings	Optional or occasional.
Location of Enterprise Architecture Board meetings	Authority Headquarters or 10 South Colonnade

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SCHEDULE 22

**CHANGE CONTROL PROCEDURE, SERVICE
REQUESTS AND PROJECTS**

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Schedule 22

Part A (*Change Control Procedure*)

1 DEFINITIONS

1.1 In Part A of this Schedule, the following definitions shall apply:

“Authority Change Manager”	the person appointed to that position by the Authority from time to time and notified in writing to the Supplier or, if no person is notified, the Authority Representative;
“Change Request”	a written request for a Contract Change which shall be substantially in the form of Annex 1;
“Change Communication”	any Change Request, Impact Assessment, Change Authorisation Note or other communication sent or required to be sent pursuant to Part A of this Schedule;
“Fast-track Change”	any Contract Change which the Parties agree to expedite in accordance with Paragraph 8;
“Impact Assessment”	an assessment of a Change Request in accordance with Paragraph 5;
“Impact Assessment Estimate”	has the meaning given in Paragraph 4.3;
“Receiving Party”	the Party which receives a proposed Contract Change; and
“Supplier Change Manager”	the person appointed to that position by the Supplier from time to time and notified in writing to the Authority or, if no person is notified, the Supplier Representative.

2 GENERAL PRINCIPLES OF CHANGE CONTROL PROCEDURE

- 2.1 Part A of this Schedule sets out the procedure for dealing with Changes.
- 2.2 Operational Changes shall be processed in accordance with Paragraph 9. If either Party is in doubt about whether a change falls within the definition of an

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Operational Change, then it must be processed as a Contract Change or a Service Change.

2.3 The Parties shall deal with Contract Change as follows:

- (a) either Party may request a Contract Change which they shall initiate by issuing a Change Request in accordance with Paragraph 4;
- (b) unless this Contract otherwise requires, the Supplier shall assess and document the potential impact of a proposed Contract Change in accordance with Paragraph 5 before the Contract Change can be either approved or implemented;
- (c) the Authority shall have the right to request amendments to a Change Request, approve it or reject it in the manner set out in Paragraph 6;
- (d) the Supplier shall have the right to reject a Change Request solely in the manner set out in Paragraph 7;
- (e) save as otherwise provided in this Contract, no proposed Contract Change shall be implemented by the Supplier until a Change Authorisation Note has been signed and issued by the Authority in accordance with Paragraph 6.2; and
- (f) if a proposed Contract Change is a Fast-track Change, it shall be processed in accordance with Paragraph 8.

2.4 To the extent that any Contract Change requires testing and/or a programme for implementation, then the Parties shall follow the procedures set out in Schedule 14 (*Testing Procedures*), and, where appropriate, the Change Authorisation Note relating to such a Contract Change shall specify Milestones and/or a Key Milestone and Milestone Date(s) in respect of such Contract Change for the purposes of such procedures.

2.5 Until a Change Authorisation Note has been signed and issued by the Authority in accordance with Paragraph 6.2, then:

- (a) unless the Authority expressly agrees (or requires) otherwise in writing, the Supplier shall continue to supply the Services in accordance with the existing terms of this Contract as if the proposed Contract Change did not apply; and
- (b) any discussions, negotiations or other communications which may take place between the Authority and the Supplier in connection with any proposed Contract Change, including the submission of any Change Communications, shall be without prejudice to each Party's other rights under this Contract.

2.6 The Supplier shall:

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (a) within 10 Working Days of the Authority's signature and issue of a Change Authorisation Note, deliver to the Authority a copy of this Contract updated to reflect all Contract Changes agreed in the relevant Change Authorisation Note and annotated with a reference to the Change Authorisation Note pursuant to which the relevant Contract Changes were agreed; and
 - (b) thereafter provide to the Authority such further copies of the updated Contract as the Authority may from time to time request.
- 2.7 Where the Authority requires a change to the CDR of an Access Circuit and the CDR will remain within the bearer capacity of the relevant Access Circuit:
 - (a) there will be no impact on the Charges; and
 - (b) the change will not have to be implemented through the Change Control Procedure (unless such change is part of a wider Change).

3 COSTS

- 3.1 Subject to Paragraphs 3.3 and 4.3, each Party shall bear its own costs in relation to the preparation and agreement of each Change Request and all Impact Assessments.
- 3.2 The cost of any Contract Change shall be calculated and charged in accordance with the principles and day rates or day costs (as applicable) set out in Schedule 15 (*Charges and Invoicing*). The Supplier shall be entitled to increase the Charges only if it can demonstrate in the Impact Assessment that the proposed Contract Change requires additional resources and, in any event, any change to the Charges resulting from a Contract Change (whether the change will cause an increase or a decrease in the Charges) will be strictly proportionate to the increase or decrease in the level of resources required for the provision of the Services as amended by the Contract Change.
- 3.3 Both Parties' costs incurred in respect of any use of this Change Control Procedure as a result of any error or Default by the Supplier shall be paid for by the Supplier.

4 CHANGE REQUEST

- 4.1 Either Party may issue a Change Request to the other Party at any time during the Term. A Change Request shall be substantially in the form of Annex 1 and state whether the Party issuing the Change Request considers the proposed Contract Change to be a Fast-track Change.
- 4.2 If the Supplier issues the Change Request, then it shall also provide an Impact Assessment to the Authority as soon as is reasonably practicable but

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

in any event within 10 Working Days of the date of issuing the Change Request.

- 4.3 If the Authority issues the Change Request, then the Supplier shall provide as soon as reasonably practical and in any event within ten (10) Working Days of the date of receiving the Change Request an estimate ("**Impact Assessment Estimate**") of any costs of preparing an Impact Assessment that cannot reasonably be provided using existing Supplier resources (for example conducting Site surveys) and the timetable for preparing it. The timetable shall provide for the completed Impact Assessment to be received by the Authority within ten (10) Working Days of acceptance of the Impact Assessment Estimate or within any longer time period agreed by the Authority.
- 4.4 If the Authority accepts an Impact Assessment Estimate then following receipt of notice of such acceptance the Supplier shall provide the completed Impact Assessment to the Authority as soon as is reasonably practicable and in any event within the period agreed in the Impact Assessment Estimate. If the Supplier requires any clarification in relation to the Change Request before it can deliver the Impact Assessment, then it shall promptly make a request for clarification to the Authority and provided that sufficient information is received by the Authority to fully understand:
- (a) The nature of the request for clarification; and
 - (b) The reasonable justification for the request;

the time period to complete the Impact Assessment shall be extended by the time taken by the Authority to provide that clarification. The Authority shall respond to the request for clarification as soon as is reasonably practicable.

5 IMPACT ASSESSMENT

- 5.1 Each Impact Assessment shall be completed in good faith and shall include:
- (a) details of the proposed Contract Change including the reason for the Contract Change; and
 - (b) details of the impact of the proposed Contract Change on:
 - (i) the Services;
 - (ii) the Optional Services (if any); and
 - (iii) the Supplier's ability to meet its other obligations under this Contract (including its security management and data processing obligations);
 - (c) any variation to the terms of this Contract that will be required as a result of that impact, including changes to:

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (i) the Services Description, the Performance Indicators and/or the Target Performance Levels;
 - (ii) the format of Authority Data, as set out in the Services Description;
 - (iii) the Milestones, Implementation Plan and any other timetable previously agreed by the Parties;
 - (iv) other services provided by third party contractors to the Authority, including any changes required by the proposed Contract Change to the Authority's IT infrastructure;
 - (d) details of the cost of implementing the proposed Contract Change;
 - (e) details of the ongoing costs required by the proposed Contract Change when implemented, including any increase or decrease in the Charges, any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party;
 - (f) a timetable for the implementation, together with any proposals for the testing of the Contract Change;
 - (g) details of how the proposed Contract Change will ensure compliance with any applicable Change in Law; and
 - (h) such other information as the Authority may reasonably request in (or in response to) the Change Request.
- 5.2 If the Contract Change involves the processing or transfer of any Personal Data outside the United Kingdom and European Economic Area, the preparation of the Impact Assessment shall also be subject to Clause 21 (*Protection of Personal Data*).
- 5.3 Subject to the provisions of Paragraph 5.4, the Authority shall review the Impact Assessment and respond to the Supplier in accordance with Paragraph 6 within 15 Working Days of receiving the Impact Assessment, it.
- 5.4 If the Authority is the Receiving Party and the Authority reasonably considers that it requires further information regarding the proposed Contract Change so that it may properly evaluate the Change Request and the Impact Assessment, then within 5 Working Days of receiving the Impact Assessment, it shall notify the Supplier of this fact and detail the further information that it requires. The Supplier shall then re-issue the relevant Impact Assessment to the Authority within 10 Working Days of receiving such notification. At the Authority's discretion, the Parties may repeat the process described in this Paragraph 5.4 until the Authority is satisfied that it has sufficient information to properly evaluate the Change Request and Impact Assessment.
- 5.5 The calculation of costs for the purposes of Paragraphs 5.1(d) and (e) shall:

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (a) be based on the the relevant provisions in Schedule 15 (Charges and Invoicing);
- (b) facilitate the Financial Transparency Objectives;
- (c) include estimated volumes of each type of resource to be employed and the applicable rate card;
- (d) include full disclosure of any assumptions underlying such Impact Assessment;
- (e) include evidence of the cost of any assets required for the Change; and
- (f) include details of any new Sub-contracts necessary to accomplish the Change.

6 AUTHORITY'S RIGHT OF APPROVAL

6.1 Within 15 Working Days of receiving the Impact Assessment from the Supplier or within 10 Working Days of receiving the further information that it may request pursuant to Paragraph 5.4, the Authority shall evaluate the Change Request and the Impact Assessment and shall do one of the following:

- (a) approve the proposed Contract Change, in which case the Parties shall follow the procedure set out in Paragraph 6.2;
- (b) in its absolute discretion reject the Contract Change, in which case it shall notify the Supplier of the rejection. The Authority shall not reject any proposed Contract Change to the extent that the Contract Change is necessary for the Supplier or the Services to comply with any Changes in Law. If the Authority does reject a Contract Change, then it shall explain its reasons in writing to the Supplier as soon as is reasonably practicable following such rejection; or
- (c) in the event that it reasonably believes that a Change Request or Impact Assessment contains errors or omissions, require the Supplier to modify the relevant document accordingly, in which event the Supplier shall make such modifications within 5 Working Days of such request. Subject to Paragraph 5.4, on receiving the modified Change Request and/or Impact Assessment, the Authority shall approve or reject the proposed Contract Change within 10 Working Days.

6.2 If the Authority approves the proposed Contract Change pursuant to Paragraph 6.1 and it has not been rejected by the Supplier in accordance with Paragraph 7, then it shall inform the Supplier and the Supplier shall prepare two copies of a Change Authorisation Note which it shall sign and deliver to

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

the Authority for its signature. Following receipt by the Authority of the Change Authorisation Note, it shall sign both copies and return one copy to the Supplier. On the Authority's signature the Change Authorisation Note shall constitute (or, where the Authority has agreed to or required the implementation of a Change prior to signature of a Change Authorisation Note, shall constitute confirmation of) a binding variation to this Contract.

- 6.3 If the Authority does not sign the Change Authorisation Note within 10 Working Days, then the Supplier shall have the right to notify the Authority and if the Authority does not sign the Change Authorisation Note within 5 Working Days of such notification, then the Supplier may refer the matter to the Expedited Dispute Timetable pursuant to the Dispute Resolution Procedure.

7 SUPPLIER'S RIGHT OF APPROVAL

- 7.1 Following an Impact Assessment, if:

- (a) the Supplier reasonably believes that any proposed Contract Change which is requested by the Authority would:
 - (i) materially and adversely affect the risks to the health and safety of any person; and/or
 - (ii) require the Services to be performed in a way that infringes any Law; and/or
- (b) the Supplier demonstrates to the Authority's reasonable satisfaction that the proposed Contract Change is technically impossible to implement and neither the Supplier Solution nor the Services Description state that the Supplier does have the technical capacity and flexibility required to implement the proposed Contract Change,

then the Supplier shall be entitled to reject the proposed Contract Change and shall notify the Authority of its reasons for doing so within 5 Working Days after the date on which it is obliged to deliver the Impact Assessment pursuant to Paragraph 4.3.

8 FAST-TRACK CHANGES

- 8.1 The Parties acknowledge that to ensure operational efficiency there may be circumstances where it is desirable to expedite the processes set out above.

- 8.2 If:

- (a) the total number of Contract Changes in relation to which this Fast-track Change procedure has been applied does not exceed 4 in any 12 month period; and
- (b) both Parties agree the value of the proposed Contract Change over the remaining Term and any period for which Termination Services

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

may be required does not exceed £50,000 and the proposed Contract Change is not significant (as determined by the Authority acting reasonably),

then the Parties shall confirm to each other in writing that they shall use the process set out in Paragraphs 4, 5, 6 and 7 but with reduced timescales, such that any period of 15 Working Days is reduced to 5 Working Days, any period of 10 Working Days is reduced to 2 Working Days and any period of 5 Working Days is reduced to 1 Working Day.

- 8.3 The Parties may agree in writing to revise the parameters set out in Paragraph 8.2 from time to time or that the Fast-track Change procedure shall be used in relation to a particular Contract Change notwithstanding that the total number of Contract Changes to which such procedure is applied will then exceed 4 in a 12 month period.

9 OPERATIONAL CHANGE PROCEDURE

- 9.1 Any Operational Changes identified by the Supplier to improve operational efficiency of the Services may be implemented by the Supplier without following the Change Control Procedure for proposed Contract Changes provided they do not:
- (a) have an impact on the business of the Authority;
 - (b) require a change to this Contract;
 - (c) have a direct impact on use of the Services; or
 - (d) involve the Authority in paying any additional Charges or other costs.
- 9.2 The Authority may request an Operational Change by submitting a written request for Operational Change ("**RFOC**") to the Supplier Representative.
- 9.3 The RFOC shall include the following details:
- (a) the proposed Operational Change; and
 - (b) the time-scale for completion of the Operational Change.
- 9.4 The Supplier shall inform the Authority of any impact on the Services that may arise from the proposed Operational Change.
- 9.5 The Supplier shall complete the Operational Change by the timescale specified for completion of the Operational Change in the RFOC, and shall promptly notify the Authority when the Operational Change is completed.

10 COMMUNICATIONS

- 10.1 For any Change Communication to be valid under Part A of this Schedule, it must be sent to either the Authority Change Manager or the Supplier Change

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Manager, as applicable. The provisions of Clause 42 (*Notices*) shall apply to a Change Communication as if it were a notice.

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 1: CHANGE REQUEST FORM

CR NO.:	TITLE:	TYPE OF CHANGE:
CONTRACT:		REQUIRED BY DATE:
ACTION:	NAME:	DATE:
RAISED BY:		
AREA(S) IMPACTED (<i>OPTIONAL FIELD</i>):		
ASSIGNED FOR IMPACT ASSESSMENT BY:		
ASSIGNED FOR IMPACT ASSESSMENT TO:		
SUPPLIER REFERENCE NO.:		
FULL DESCRIPTION OF REQUESTED CONTRACT CHANGE (INCLUDING PROPOSED CHANGES TO THE WORDING OF THE CONTRACT):		
DETAILS OF ANY PROPOSED ALTERNATIVE SCENARIOS:		
REASONS FOR AND BENEFITS AND DISADVANTAGES OF REQUESTED CONTRACT CHANGE:		
SIGNATURE OF REQUESTING CHANGE OWNER:		
DATE OF REQUEST:		

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 2: CHANGE AUTHORISATION NOTE

CR NO.:	TITLE:	DATE RAISED:
CONTRACT:	TYPE OF CHANGE:	REQUIRED BY DATE:
[KEY MILESTONE DATE: <i>[if any]</i>]		
DETAILED DESCRIPTION OF CONTRACT CHANGE FOR WHICH IMPACT ASSESSMENT IS BEING PREPARED AND WORDING OF RELATED CHANGES TO THE CONTRACT:		
PROPOSED ADJUSTMENT TO THE CHARGES RESULTING FROM THE CONTRACT CHANGE:		
DETAILS OF PROPOSED ONE-OFF ADDITIONAL CHARGES AND MEANS FOR DETERMINING THESE (E.G. FIXED PRICE BASIS):		
SIGNED ON BEHALF OF THE AUTHORITY:		SIGNED ON BEHALF OF THE SUPPLIER:
Signature:_____		Signature:_____
Name:_____		Name:_____
Position:_____		Position:_____
Date:_____		Date:_____

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Part B (Service Requests and Projects)**1 DEFINITIONS**

1.1 In Part B of this Schedule, the following definitions shall apply:

“Business Hours”	means hours between 9am and 5.30pm on any Working Day;
“Outline Project Plan”	means in relation to a Project, the plan set out in section 6 of the relevant Project Work Order;
“Project Plan”	a statement of how and when a Project's objectives are to be achieved, by showing the major products, Milestones, activities, deliverables and resources required on the Project;
“Project Proposal”	has the meaning given to it in Paragraph 5.1 of Part B of this Schedule;
“Project Request”	means a request from the Authority in relation to a proposed Project in accordance with Paragraph 4.2 of this Part B of this Schedule;
“Project Work Order Meeting”	has the meaning given to it in Paragraph 6.4 of Part B of this Schedule;
“Request”	a Service Request and/or a Project Request;
“Service Request”	has the meaning given to it in Paragraph 3 of Part B of this Schedule.

2 INTRODUCTION

2.1 Part B of this Schedule sets out the procedures for dealing with:

2.1.1 Service Requests; and

2.1.2 Project Requests.

2.2 If the Parties' agreement of any Project Work Order or Service Request (including any subsequent changes to them), shall require a Change to be made to the Contract, then in accordance with Clause 13.1 such Changes shall be subject to the Change Control Procedure.

2.3 The Authority shall provide the Supplier with the details of the individuals who are authorised by the Authority to raise and approve Requests and shall notify the Supplier of any changes made by the Authority to such details during the Term.

2.4 The Supplier shall:

2.4.1 respond to a Request in accordance with paragraphs 3.3 to 3.8 inclusive and 4.4 to 4.7 inclusive of this Part B; and

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 2.4.2 deliver, perform or otherwise implement the Services set out in the Request,
- in a timely manner consistent with the relevant lead times agreed in accordance with Part B of this Schedule.
- 2.5 The procedures in Part B of this Schedule shall not be used to request Changes which shall be dealt with in accordance with Clause 13.1 (Change Control Procedure).
- 2.6 A Request that relates to a Project Work Order shall only be valid when the Demand Management System indicates it has been authorised (or otherwise, it is signed by an authorised individual as notified to the Supplier by the Authority in accordance with paragraph 2.3).
- 2.7 Each Party shall be responsible for its own costs incurred in proposing, preparing, discussing, negotiating and agreeing any Request.
- 2.8 Any Charges applicable to any Request that are agreed by the Authority in accordance with this Schedule shall be payable in accordance with Schedule 15 (Charges and Invoicing).
- 2.9 The Supplier acknowledges that the Authority is not obliged to raise Project Requests and provides no guarantee to the Supplier on the volume, value or quantity of any Projects that the Authority may require under this Contract (if any) and that nothing shall prevent the Authority from receiving services that are the same or similar to any services that may be covered by a Project from any third party.
- 2.10 The Supplier shall ensure that:
- 2.10.1 all the Registers, as well as any including asset, licensing, warranty and/or Configuration Management information are updated by the end of the next Working Day following the installation, removal or movement to reflect the changes which have resulted from the installation, removal or movement of assets and initiation of Services; and
- 2.10.2 all Requests related activities are co-ordinated to optimise the use of resources.
- 2.11 Requests shall be submitted and processed via and within the ITSM Toolset unless otherwise agreed by the Authority.

3 SERVICE REQUESTS

- 3.1 A Service Request enables the Authority to order Catalogue Items from the Product and Service Catalogue where no changes are required to the Catalogue Item(s) and the lead time stated within the Product and Service Catalogue.

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 3.2 Each Service Request submitted by the Authority shall as a minimum:
- 3.2.1 state the type and quantity of the Catalogue Item(s) which the Authority wishes to order;
 - 3.2.2 Not Used.
 - 3.2.3 (where relevant) state the location for delivery of the Catalogue Item(s);
 - 3.2.4 include a valid cost centre, location information, business area, and contact point information; and
 - 3.2.5 include such other information available to or in the possession of the Authority that is reasonably necessary for the Supplier to perform the Service Request and fulfil the relevant Catalogue Item(s).
- 3.3 Upon receipt of the Service Request, the Supplier shall promptly notify the Authority of any non-compliance with the provisions of Paragraph 3.2; otherwise, it shall be deemed to constitute an agreed Service Request within the timescale agreed under the Request Fulfilment Process and/or the Product & Service Catalogue Management Process (or if no timescale is so specified then within four (4) Business Hours of the Service Request being submitted).
- 3.4 If the Service Request submitted to the Supplier in accordance with Paragraph 3.1 does not, in the reasonable opinion of the Supplier, comply with the provisions of Paragraph 3.2, the Supplier shall notify the Authority within the timescale agreed under the Request Fulfilment Process and/or the Product & Service Catalogue Management Process (or if no timescale is so specified then within four (4) Business Hours of the Service Request being submitted) of receipt of the Service Request and explain its reasons for rejecting the relevant Service Request.
- 3.5 In relation to each Service Request accepted in accordance with paragraph 3.3:
- 3.5.1 the Supplier shall achieve the date for the fulfilment of the Catalogue Item(s) in accordance with the applicable lead time set out in the Product and Service Catalogue;
 - 3.5.2 lead times set out in the Product and Service Catalogue commence from the time the Authority submits the Service Request; and
 - 3.5.3 if there are any Catalogue Item Charges applicable to the Catalogue Item(s) set out in the Service Request these shall be payable in accordance with Schedule 15 (Charges and Invoicing) after the relevant Services are received by the Authority.
- 3.6 The Supplier shall provide regular status updates to the Authority for the

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

purpose of tracking, managing and closing Service Requests.

- 3.7 In the event that any Service Requests are cancelled by the Authority whilst the Supplier is delivering the Service Request but before completion of such Service Request:

3.7.1 the Supplier shall:

- (a) notify the Authority in writing of any costs incurred by the Supplier in fulfilling the Service Request up to and including the date of cancellation and/or any direct and unavoidable losses and/or expenses incurred as a result of the cancellation of such Service Request; and
- (b) cooperate with the Authority and take all reasonable steps to eliminate or, if this is not possible, mitigate any costs, losses and/or expenses that it incurs as a result of the Authority's cancellation of a Service Request,

and provide to the Authority such documentation that the Authority shall reasonably require to evidence the same; and

- 3.7.2 subject to the Supplier complying with the provisions of paragraph 3.7.1 above, the Authority shall pay any such costs, losses and/or expenses incurred by the Supplier as a result of the Authority's cancellation of a Service Request in accordance with the provisions of Clause 15 (Charges and Invoicing) and Schedule 15 (Charges and Invoicing).

- 3.8 The Supplier shall reasonably co-operate and work closely with Other Suppliers in satisfying any Service Requests that may impact across any information and communication services being delivered to the Authority and in so doing shall comply with the co-operation and collaboration requirements set out in Clause 5.5(f) and in Schedule 2 (Services Description) for the delivery of such Service Requests.

4 PROJECTS

- 4.1 The Authority may issue a Project Request to the Supplier in accordance with the process set out in this Paragraph 4 (the "**Project Initiation Process**").

- 4.2 A Project Request shall include the following (to the extent relevant):

- 4.2.1 a brief context, identifying the positioning of the intended Project in the Authority's IT strategy, targets, timescales and objectives;
- 4.2.2 a detailed statement of the Authority's requirements for the intended Project (including scope);
- 4.2.3 the objectives and goals of the intended Project and its contribution to the Authority's business objectives;

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 4.2.4 the charging basis proposed by the Authority for the intended Project (which may be Milestone Payments, fixed price, time and materials or capped time and materials) by reference to the relevant paragraph of Schedule 15 (Charges and Invoicing) and any guidance, which the Authority wishes the Supplier to consider, in respect of pricing mechanisms;
- 4.2.5 details of any standard estimating tool that the Authority proposes be used by the Supplier for estimating resources;
- 4.2.6 any known technical, time or any other constraints;
- 4.2.7 key assumptions and any known risks;
- 4.2.8 whether Testing is required in accordance with Schedule 14 (Testing Procedures) or approval of Documentary Deliverables in accordance with the Document Approval Procedure;
- 4.2.9 the proposed Milestones and proposed Test Success Criteria for the intended Project;
- 4.2.10 details of the Project Test Strategy (if any) relevant to the intended Project; and
- 4.2.11 the desired level of progress reporting.
- 4.3 The Authority may at its reasonable discretion, at any time prior to the execution of a Project Work Order in accordance with paragraph 6.1 below, terminate the Project Initiation Process for such intended Project by providing written notice to that effect to the Supplier.
- 4.4 If in the reasonable opinion of the Supplier, the Project Request fails to comply with the requirements of paragraph 4 the Supplier shall notify the Authority in writing and explain its reasons within five (5) Working Days of receipt of the Project Request and the Parties shall seek to agree the most appropriate means of remedying such failures.

5 PROJECT PROPOSALS

- 5.1 The Supplier shall provide to the Authority in response to each Project Request received by the Supplier which complies with the requirements of paragraph 4.2:
 - 5.1.1 a Proposal Document; or
 - 5.1.2 where agreed with the Authority in advance, a draft Project Work Order prepared in accordance with paragraph 5,
 (a "**Project Proposal**") within twenty (20) Working Days or such other time period as is reasonably requested by the Authority and agreed by the Authority and the Supplier (taking into account the nature and complexity of

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

the Project Request in question).

- 5.2 Each Project Proposal shall be clear and unambiguous and set out all information necessary, and in sufficient detail, to allow a preliminary assessment by the Authority of the relevant intended Project, including the following information as a minimum:
- 5.2.1 outline approach, work breakdown structure (i.e. the appropriate Milestones (including any Milestones which attract Milestone Payments) key Deliverables, timescales and estimated number of each type of resource required, based on any estimating tool referred to in paragraph 4.2.5) and Project Implementation Plan. Wherever possible, the Supplier shall use Catalogue Items where relevant to the Project;
 - 5.2.2 an Outline Project Plan;
 - 5.2.3 details of any required third party service in relation to the intended Project including:
 - (a) the nature of the required third party service and anticipated charges; and
 - (b) the identity of the proposed third party supplier who shall provide the required third party service;
 - 5.2.4 key assumptions (including any cost assumptions) and anticipated risks;
 - 5.2.5 any additional Authority Responsibilities specific to the intended Project (if any);
 - 5.2.6 an assessment as to whether:
 - (a) any element of the Services which would be required in respect of that intended Project are already being provided by the Supplier under this Contract; and
 - (b) where the result of the Supplier's assessment is that the intended Project would be best delivered by an alternative means (for example, by a Service Request), details of the Supplier's recommendations as to the most appropriate means of delivery for the intended Project;
 - 5.2.7 if the Supplier reasonably determines that Testing or Approval of Documentary Deliverables in accordance with the Document Approval Procedure will be required in respect of the intended Project (whether or not the Authority has identified this itself in the Project Request);
 - 5.2.8 the charges proposed by the Supplier with reference to the prices set out in the relevant paragraph of Schedule 15 (Charges and

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Invoicing) which would be payable by the Authority for undertaking the intended Project in accordance with the charging basis proposed by the Authority in the Project Request as set out in paragraph 4.2.4 above. Such charges shall include the costs of complying with the Test Success Criteria;

- 5.2.9 any proposals in respect of funding or alternative pricing or new pricing mechanisms that the Supplier wishes the Authority to consider;
 - 5.2.10 details of any proposed Reimbursable Expenses;
 - 5.2.11 comments upon the Test Success Criteria (if any) proposed by the Authority for the intended Project;
 - 5.2.12 outline details of the possible impact of the intended Project upon major works (for example implementation of the Contract, exit or other Projects) and/or of major works upon the intended Project together with details of the Supplier's recommendations for addressing such possible impact.
- 5.3 Where in the reasonable opinion of the Authority, any Project Proposal fails to set out in sufficient detail the information required by paragraph 5.2 to enable the Authority to carry out its initial assessment of an intended Project: the Supplier shall, to the extent reasonably practicable, remedy any such failing within such time-scales as are reasonably requested by the Authority, or in the absence of such request, five (5) Working Days.

6 PROJECT WORK ORDERS

- 6.1 Following review of a Project Proposal, the Authority shall within a reasonable period, and in any event, within thirty (30) days of receipt of the Project Proposal from the Supplier, notify the Supplier whether it wishes to consider the Project further, and if so shall require the Supplier to produce a draft Project Work Order within ten (10) Working Days of the Authority's notice (or such other time period as may be agreed by the Parties), for agreement by the Authority.
- 6.2 As part of the production of each such Project Work Order, the Parties shall also seek to collaborate and cooperate with Other Suppliers to establish the impact of the intended Project on Other Suppliers, and / or other Project or intended Project and adjust the intended Project accordingly to reasonably take into account any such impact.
- 6.3 Each Project Work Order shall, unless otherwise agreed by the Parties, be in accordance with the structure as outlined in Annex 1.
- 6.4 Following production of a draft Project Work Order in accordance with paragraph 6.2, and where requested by the Authority, the Parties shall jointly establish (as appropriate) a project board which shall meet as soon as

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

practicable on a date agreed between the Parties ("**Project Work Order Meeting**"). The project board shall establish the appropriate governance, risk management processes and any specific reporting requirements for each Project. At the Project Work Order Meeting the Parties shall further consider the intended Project and shall review the information set out in the draft Project Work Order with a view to agreeing the final agreed contents of the Project Work Order in question, together with any other issues relating to the intended Project as are reasonably raised by each Party.

- 6.5 At each Project Work Order Meeting the Parties may require changes to a relevant draft Project Work Order to be considered at a subsequent Project Work Order Meeting. In these circumstances the Supplier shall submit a revised Project Work Order as soon as reasonably practicable after the meeting. This process shall be repeated as necessary until the draft Project Work Order is agreed by the Parties or the Authority cancels its requirement for the Project Work Order.

7 PROJECT COMMITMENT

- 7.1 For the avoidance of doubt, if the Parties agree the contents of the draft Project Work Order pursuant to paragraphs 5.4 or 5.5 above, the Supplier shall prepare two copies of a Project Work Order which it shall sign and deliver to the Authority for its signature. Following receipt by the Authority of the Project Work Order it shall sign both copies and return one copy to the Supplier. On the Authority's signature the Project Work Order shall be binding on both Parties.
- 7.2 Neither Party shall become contractually committed in respect of any Project unless and until such time as a Project Work Order has been executed by both Parties in accordance with paragraph 7.1 above.

8 PROJECT COMMENCEMENT

- 8.1 Following execution of the Project Work Order by both Parties, a Project start meeting shall take place (unless the Parties agree otherwise) between the Parties prior to any work being undertaken on that Project.

9 CHANGES TO AGREED PROJECT WORK ORDERS

- 9.1 Following the agreement of any Project Work Order, any changes to such Project Work Order proposed by either Party shall only become effective if the change has been agreed by both Parties in writing.
- 9.2 The mechanism for changes to Project Work Orders shall be for the Supplier to create a revised version of the relevant Project Work Order, including a statement that such revised version supersedes any previous version. The Supplier shall prepare two copies of the revised Project Work Order which it shall sign and deliver to the Authority for its signature. Following receipt by the Authority of the revised Project Work Order it shall sign both copies and return one copy to the Supplier. On the Authority's signature the revised

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Project Work Order shall be binding on both Parties.

- 9.3 The Authority may, by giving the Supplier prior written notice, require the termination of a Project after it has commenced, in which case the Parties' obligations in respect of the remaining Services shall continue unaffected and a Termination Payment shall only be payable by the Authority if applicable in accordance with Schedule 16 (Payments on Termination).
- 9.4 Termination of a Project in accordance with paragraph 8.3 shall be without prejudice to any right of action or remedy of either Party which has accrued or which subsequently accrues.

10 SUB-CONTRACTORS AND SUPPLIERS

- 10.1 The Supplier may engage any Sub-Contractor or third party supplier in relation to any Project subject to the terms of this Schedule and in accordance with this Contract.
- 10.2 In respect of each Sub-Contractor or third party supplier engaged by the Supplier on its own accord in relation to a Project the Supplier shall, at no cost to the Authority, ensure that prior to the commencement of any work by that Sub-Contractor or third party supplier in relation to the Project such Sub-Contractor or third party supplier is given appropriate information in relation to the Project which shall include, at a minimum, the following information but only where such information is relevant to the work to be undertaken by the Sub-Contractor or third party supplier:
- 10.2.1 an overview of the Supplier's and Authority's respective organisations including background and position in the market (in the case of the Supplier) and the political landscape (in the case of the Authority);
 - 10.2.2 an overview of the relevant Authority's organisation(s) to which the Project relates and/or impacts;
 - 10.2.3 an introduction to the Project itself, including the relevant background and its intended contribution to the Authority's business objectives;
 - 10.2.4 the policies and procedures that are relevant to the Project;
 - 10.2.5 an overview of the composition of the Project team (including the different roles of each member or categories of members) and key stakeholders;
 - 10.2.6 the specific roles, responsibilities and objectives of the Sub-Contractor or third party supplier in relation to the Project (including any relevant background material);
 - 10.2.7 any relevant administrative requirements (e.g. time sheets, status reports and project meetings); and

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 10.2.8 any relevant Authority or Supplier policies or procedures specific to the Sub-Contractor's or third party supplier's role.

11 CONFLICTS OF INTEREST

- 11.1 Where the provision or planning of any Project or Service Request involves the selection of, or advice upon the selection of, alternative courses of action (including refraining from a particular course of action) or the acquisition, or advice upon the acquisition of goods, services and rights, the Supplier shall make such selection or acquisition or give such advice in an impartial, independent and unbiased manner and in the best interests of the Authority.
- 11.2 If the Supplier becomes aware of any actual or potential conflict of interest in relation to any Project or Service Request (whether such existed before the Commencement Date or thereafter) it shall, without undue delay, notify the Authority in writing providing full particulars of the actual or potential conflict together with any additional information which the Authority may require in connection with such matter.

12 AUDIT OF PROJECT OR SERVICE REQUESTS

- 12.1 The Authority shall have the right to audit any Project or Service Request consistent with the provisions set out in Part C (Audit Rights) of Schedule 19 (Financial Reports and Audit Rights).
- 12.2 The Authority reserves the right to verify throughout each Project or Service Request that the level of skill and experience of individuals assigned remains consistent with the grade associated with the Supplier Personnel upon which the Supplier bases its charges for the Project or Service Request prior to inception of the Project or Service Request. The Supplier shall provide to the Authority such information as the Authority may reasonably request to enable it to exercise its rights under this paragraph 12.2.

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 1: PROJECT WORK ORDER TEMPLATE**1 DESCRIPTION AND CONSEQUENCES OF PROJECT WORK ORDER**

PWO Title			
PWO Number		Version No.	
Business Area	<HMCTS/HMPPS etc.>	CTS Demand Ref.	
Date of Request		Date Required By	
Reason for Project			
Project Summary			
Related Projects	<Enter any related PWO numbers>		
Key People			
	Name	Email	Phone Number
Business SPOC #1			
Business SPOC #2			
Demand Manager			
Product Manager			
Supplier Lead			
Budget Holder			
Cost Centre Code		Entity Code	
Charges	Implementation	On-going Service	Totals
Professional Services			
Standard Items			
Non-Standard Items			
Contingency			
Totals			
Critical Dates			
Decision by Date		Expiry Date	
Comments on Critical Date			

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

2 INTRODUCTION

- 2.1 This Project Work Order ("PWO") constitutes an addition to the Contract for provision of WAN Services entered into on [Effective Date] (as amended by the Parties from time to time) between the Authority and the Supplier (the "Contract").
- 2.2 The Parties agree that Section 1 is included to assist the understanding of this PWO prior to signature and shall not form part of the Contract nor affect the interpretation of the Contract or this PWO.
- 2.3 Save as may be otherwise provided in this PWO, the Contract terms shall apply to the Project undertaken by the Supplier pursuant to this PWO and all provisions in the Contract applicable to provision of Services will apply mutatis mutandis to the Services provided under this PWO.
- 2.4 In the event and only to the extent of any inconsistency between any agreed term of this PWO and any term of the Contract then the term of this PWO shall prevail.
- 2.5 In this PWO, references to "Sections" are to sections contained within this PWO.
- 2.6 All prices and charges set out in this PWO are exclusive of VAT.

3 CHANGES TO THIS PWO

- 3.1 For the avoidance of doubt, all Changes shall be implemented by the Parties in accordance with the Change Control Procedure.
- 3.2 Following the agreement of any Project Work Order, any changes to such Project Work Order proposed by either Party shall only become effective provided that a revised version of this Project Work Order has agreed by both Parties in writing in accordance with the procedure set out in paragraph 8 of Part B of Schedule 22 (Change Control Procedure, Service Requests and Projects).
- 3.3 The Parties hereby agree to this revised issue of this PWO, which shall supersede all previously executed versions of this PWO with effect from the date of signing by both Parties of this revised PWO. The table below provides a summary of all revision levels of this PWO that have been executed by the Parties:

Version No.	Effective Date	Summary of changes incorporated into this Version
1.0		Original issue.

4 REQUIREMENTS

[Free flow text area to capture the high-level Authority requirements and reference to any detailed requirements specification/documents etc.]

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

5 SPECIFICATION

- 5.1 The specification of the Project to be delivered under this PWO is detailed in Appendix 1 and summarised here as the following key deliverables (“Deliverables”);
 - 5.1.1 <Enter Deliverable(s)>
- 5.2 Assumptions
 - 5.2.1 <Enter Assumption(s)>
- 5.3 Exclusions
 - 5.3.1 <Enter Exclusion(s)>
- 5.4 Dependencies
 - 5.4.1 <Enter Dependencies>
- 5.5 Authority Responsibilities
 - 5.5.1 <Enter Authority Responsibilities>
- 5.6 Risks and Mitigations
 - 5.6.1 <Enter Risks and Mitigations>

6 PROJECT PLAN

- 6.1 A detailed Project Plan and a Project Initiation Document will be agreed between the Parties following commencement of the Project.
- 6.2 Any changes or additions to the Project Plan, including Milestone Dates will require the written agreement of both Parties, acting reasonably and in good faith to make such changes.
- 6.3 The high-level Milestones for the Project are set out below:

[Provide an Outline Project Plan (in substantively the format set out in the plan template below) which will be developed over time into the Project Plan.]

Milestone	Deliverables (bulleted list showing all Deliverables (and associated tasks) required for each Milestone)	Duration (Working Days/ Months)	Milestone Completion Date
M1			
M2			
M3			
M4			

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

7 PRICE AND PAYMENT

- 7.1 The total price for the products and services set out in this PWO is £xx,xxx.xx (excluding VAT) and is provided on a [Fixed Price/Time and Materials/Capped Time and Materials] basis.
- 7.2 A summary breakdown of the one-off implementation charges pursuant to this PWO are as follows:

Item	Charge	Contingency	Sub-Total
Professional Services			
Standard Service Items			
Non-Standard Items			
Totals			

7.3 Milestone Payments

Milestone Payment	Details	Payment	Linked Milestone(s)
MP1			
MP2			
MP3			

- 7.3.1 The Supplier shall issue a Milestone Achievement Certificate (and providing where applicable, associated and approved timesheets) for each completed Milestone and will detail the Supplier's confirmation that the Deliverables in the applicable Milestone have met the agreed Test Success Criteria and unless otherwise notified by the Authority within ten (10) working days shall be deemed as accepted by the Authority.

7.4 On-going Service Charge

- 7.4.1 The Authority shall be liable for the service charge of £x,xxx,xxx.00 from successful completion of the Deliverables set out in Section 5 of this PWO.

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

7.4.2 The service charge consists of 12 calendar monthly payments (pro rata) of £x,xxx,xxx.00 and shall be invoiced monthly in arrears against this PWO. Thereafter the Authority shall be invoiced for the monthly service charge against the <Insert Reference to Standard Invoice>.

7.5 A detailed breakdown of all the associated charges pursuant to this PWO are set out in Appendix 2 to this PWO.

8 TERMINATION

[Insert, where appropriate, the Project exit arrangements, in the event the Project is terminated prior to completion.]

9 SUB-CONTRACTORS AND THIRD-PARTY SUPPLIERS

[Insert, where appropriate, details of any required third-party service to be used in relation to the Project along with the identity of the third-party supplier and the applicable charges calculated in accordance with Schedule 15 (Charges and Invoicing) of the Contract. If new hardware/software then warranty, sourcing decision and impact on standard catalogue are also to be included.]

10 APPLICATION OF THIS PROJECT WORK ORDER POST COMPLETION

[Insert details of any terms of this Project Work Order which will continue in/come into force following completion of the Project (e.g. any ongoing charges and the period for which the service is to be provided (if agreed to be charged within an PWO))]

11 EXIT AND/OR CONTRACT IMPLEMENTATION IMPACT

[This will be required where contracts or large-scale projects may have an impact on the wider programme such as exit and Contract Implementation. If nothing applicable, then it should state "Not applicable to this PWO."]

12 OTHER PROVISIONS

[Insert details of other provisions not covered above which may be required for a Project (to the extent not covered by the Contract Terms) otherwise state "Not applicable to this PWO."]

13 APPROVALS

Approvals to be confirmed within the Demand Management System or otherwise in writing (e.g. by e-mail).

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Appendix 1 – Service and Technical Specification

[Free flow text area for the Supplier to document its service and technical solution to meet the Authority requirements.]

Appendix 2 – Charge Breakdown

[The following are example tables, the Supplier is free to suitably document a reasonable level of breakdown of all the Charges pursuant to this PWO in such a manner that the Authority is able to perform Value for Money assessments.]

Table A1 – Professional Services

Role Code	Activity Description	Day Rate	No. Man-days	Total Charge
			Total	£xx,xxx.xx

Table A2 – Standard Catalogue Items

Item Description	Unit Charge	Qty	Total Charge
		Total	£xx,xxx.xx

Table A3 – Non-Standard Items

Item Description	Unit Charge	Qty	Total Charge

SCHEDULE 22 (CHANGE CONTROL PROCEDURE, SERVICE REQUESTS & PROJECTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Total			£xx,xxx.xx

Table A4 – Delay Payments (if applicable)

Item Description	Delay Payment amount	Qty	Total Charge
Total			£xx,xxx.xx

SCHEDULE 23 (DISPUTE RESOLUTION PROCEDURE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 23

DISPUTE RESOLUTION PROCEDURE

SCHEDULE 23 (DISPUTE RESOLUTION PROCEDURE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 23 (*Dispute Resolution Procedure*)**1 DEFINITIONS**

1.1 In this Schedule, the following definitions shall apply:

“CEDR”	the Centre for Effective Dispute Resolution of International Dispute Resolution Centre 1 Patternoster Lane, St Paul’s, London, EC4M 7BQ;
“Counter Notice”	has the meaning given in Paragraph 7.2;
“Expert”	in relation to a Dispute, a person appointed in accordance with Paragraph 6.2 to act as an expert in relation to that Dispute;
“Expert Determination”	determination by an Expert in accordance with Paragraph 6;
“Mediation Notice”	has the meaning given in Paragraph 4.2;
“Mediator”	the independent third party appointed in accordance with Paragraph 5.2 to mediate a Dispute;
“Multi-Party Dispute”	a Dispute which involves the Parties and one or more Related Third Parties;
“Multi-Party Dispute Representatives”	has the meaning given in Paragraph 9.6;
“Multi-Party Dispute Resolution Board”	has the meaning given in Paragraph 9.6;
“Related Third Party”	a party to: (a) another contract with the Authority or the Supplier which is relevant to this Contract; or (b) a Sub-contract; and
“Supplier Request”	a notice served by the Supplier requesting that the Dispute be treated as a Multi-Party Dispute, setting out its grounds for that request and specifying each Related Third Party that it believes

SCHEDULE 23 (DISPUTE RESOLUTION PROCEDURE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

should be involved in the Multi-Dispute Resolution Procedure in respect of that Dispute.

2 DISPUTE NOTICES**2.1** If a Dispute arises then:

- (a) the Authority Representative and the Supplier Representative shall attempt in good faith to resolve the Dispute; and
- (b) if such attempts are not successful within a reasonable period, not being longer than 20 Working Days, either Party may issue to the other a Dispute Notice.

2.2 A Dispute Notice:

- (a) shall set out:
 - (i) the material particulars of the Dispute;
 - (ii) the reasons why the Party serving the Dispute Notice believes that the Dispute has arisen; and
 - (iii) if the Party serving the Dispute Notice believes that the Dispute should be dealt with under the Expedited Dispute Timetable, the reason why; and
- (b) may specify in accordance with the requirements of Paragraphs 9.2 and 9.3 that the Party issuing the Dispute Notice has determined (in the case of the Authority) or considers (in the case of the Supplier) that the Dispute is a Multi-Party Dispute, in which case Paragraph 2.3 shall apply.

2.3 If a Dispute Notice specifies that the Dispute has been determined or is considered to be a Multi-Party Dispute pursuant to Paragraph 2.2(b), then:

- (a) if it is served by the Authority it shall be treated as a Multi-Party Procedure Initiation Notice; and
- (b) if it is served by the Supplier it shall be treated as a Supplier Request,

and in each case the provisions of Paragraph 9 shall apply.

2.4 Subject to Paragraphs 2.5 and 3.2 and so long as the Authority has not served a Multi-Party Procedure Initiation Notice in respect of the relevant Dispute, following the issue of a Dispute Notice the Parties shall seek to resolve the Dispute:

- (a) first by commercial negotiation (as prescribed in Paragraph 4);
- (b) then, if either Party serves a Mediation Notice, by mediation (as prescribed in Paragraph 5); and

SCHEDULE 23 (DISPUTE RESOLUTION PROCEDURE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (c) lastly by recourse to arbitration (as prescribed in Paragraph 7) or litigation (in accordance with Clause 44 (*Governing Law and Jurisdiction*)).
- 2.5 Specific issues shall be referred to Expert Determination (as prescribed in Paragraph 6) where specified under the provisions of this Contract and may also be referred to Expert Determination where otherwise appropriate as specified in Paragraph 6.1.
- 2.6 Unless agreed otherwise in writing, the Parties shall continue to comply with their respective obligations under this Contract regardless of the nature of the Dispute and notwithstanding any issue of a Dispute Notice or a Multi-Party Procedure Initiation Notice or proceedings under Paragraph 8 (*Urgent Relief*).
- 3 EXPEDITED DISPUTE TIMETABLE**
 - 3.1 In exceptional circumstances where the use of the times in this Schedule would be unreasonable, including (by way of example) where one Party would be materially disadvantaged by a delay in resolving the Dispute, the Parties may agree to use the Expedited Dispute Timetable. If the Parties are unable to reach agreement on whether to use the Expedited Dispute Timetable within 5 Working Days of the issue of a Dispute Notice, the use of the Expedited Dispute Timetable shall be at the sole discretion of the Authority.
 - 3.2 If the Expedited Dispute Timetable is to be used pursuant to the provisions of Paragraph 3.1 or is otherwise specified under the provisions of this Contract, then the following periods of time shall apply in lieu of the time periods specified in the applicable Paragraphs:
 - (a) in Paragraph 4.2(c), 10 Working Days;
 - (b) in Paragraph 5.2, 10 Working Days;
 - (c) in Paragraph 6.2, 5 Working Days; and
 - (d) in Paragraph 7.2, 10 Working Days.
 - 3.3 If at any point it becomes clear that an applicable deadline cannot be met or has passed, the Parties may (but shall be under no obligation to) agree in writing to extend the deadline. If the Parties fail to agree within 2 Working Days after the deadline has passed, the Authority may set a revised deadline provided that it is no less than 5 Working Days before the end of the period of time specified in the applicable Paragraphs (or 2 Working Days in the case of Paragraph 6.2). Any agreed extension shall have the effect of delaying the start of the subsequent stages by the period agreed in the extension. If the Authority fails to set such a revised deadline then the use of the Expedited Dispute Timetable shall cease and the normal time periods shall apply from that point onwards.

SCHEDULE 23 (DISPUTE RESOLUTION PROCEDURE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

4 COMMERCIAL NEGOTIATION

4.1 Following the service of a Dispute Notice, then, so long as the Authority has not served a Multi-Party Procedure Initiation Notice in respect of the relevant Dispute, the Authority and the Supplier shall make reasonable endeavours to resolve the Dispute as soon as possible by commercial negotiation between the Authority's Commercial representative and the Supplier's Commercial representative, each of whom shall be of a suitable level of seniority to finalise any agreement to settle the Dispute.

4.2 If:

- (a) either Party is of the reasonable opinion that the resolution of a Dispute by commercial negotiation, or the continuance of commercial negotiation, will not result in an appropriate solution;
- (b) the Parties have already held discussions of a nature and intent (or otherwise were conducted in the spirit) that would equate to the conduct of commercial negotiation in accordance with this Paragraph 4; or
- (c) the Parties have not settled the Dispute in accordance with Paragraph 4.1 within 30 Working Days of service of the Dispute Notice,

either Party may serve a written notice to proceed to mediation in accordance with Paragraph 5 (a "**Mediation Notice**").

5 MEDIATION

5.1 If a Mediation Notice is served, the Parties shall attempt to resolve the dispute in accordance with the version of CEDR's Model Mediation Procedure which is current at the time the Mediation Notice is served (or such other version as the Parties may agree).

5.2 If the Parties are unable to agree on the joint appointment of an independent person to mediate the Dispute within 20 Working Days from (and including) the service of a Mediation Notice then either Party may apply to CEDR to nominate such a person.

5.3 If the Parties are unable to reach a settlement in the negotiations at the mediation, and only if both Parties so request and the Mediator agrees, the Mediator shall produce for the Parties a non-binding recommendation on terms of settlement. This shall not attempt to anticipate what a court might order but shall set out what the Mediator suggests are appropriate settlement terms in all of the circumstances.

5.4 Any settlement reached in the mediation shall not be legally binding until it has been reduced to writing and signed by, or on behalf of, the Parties (in accordance with the Change Control Procedure where appropriate). The Mediator shall assist the Parties in recording the outcome of the mediation.

SCHEDULE 23 (DISPUTE RESOLUTION PROCEDURE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

6 EXPERT DETERMINATION

- 6.1 If a Dispute relates to any aspect of the technology underlying the provision of the Services or otherwise relates to a technical matter of an IT, accounting or financing nature and the Dispute has not been resolved by commercial negotiation in accordance with Paragraph 4 or, if applicable, mediation in accordance with Paragraph 5, then either Party may by written notice to the other request (agreement to which request shall not be unreasonably withheld or delayed) that the Dispute be referred to an expert for determination.
- 6.2 The expert shall be appointed by agreement in writing between the Parties, but in the event of a failure to agree within 10 Working Days of the relevant request made pursuant to Paragraph 6.1, or if the person appointed is unable or unwilling to act, the expert shall be appointed:
- (a) if the Dispute relates to any aspect of the technology underlying the provision of the Services or a matter of an IT technical nature, on the instructions of the President of the British Computer Society (or any other association that has replaced the British Computer Society);
 - (b) if the Dispute relates to a matter of a financial technical nature, on the instructions of the President of the Institute of Chartered Accountants of England and Wales; or
 - (c) if the Dispute relates to a matter of a technical nature not falling within Paragraphs 6.2(a) or (b), on the instructions of the president (or equivalent) of:
 - (i) an appropriate body agreed between the Parties; or
 - (ii) if the Parties do not reach agreement on the relevant body within 15 Working Days of the relevant request made pursuant to Paragraph 6.1, such body as may be specified by the President of the Law Society on application by either Party.
- 6.3 The Expert shall act on the following basis:
- (a) he/she shall act as an expert and not as an arbitrator and shall act fairly and impartially;
 - (b) the Expert's determination shall (in the absence of a material failure to follow the agreed procedures) be final and binding on the Parties;
 - (c) the Expert shall decide the procedure to be followed in the determination and shall be requested to make his/her determination within 30 Working Days of his appointment or as soon as reasonably practicable thereafter and the Parties shall assist and provide the documentation that the Expert requires for the purpose of the determination;

SCHEDULE 23 (DISPUTE RESOLUTION PROCEDURE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (d) any amount payable by one Party to another as a result of the Expert's determination shall be due and payable within 20 Working Days of the Expert's determination being notified to the Parties;
- (e) the process shall be conducted in private and shall be confidential;
and
- (f) the Expert shall determine how and by whom the costs of the determination, including his/her fees and expenses, are to be paid.

SCHEDULE 23 (DISPUTE RESOLUTION PROCEDURE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

7 ARBITRATION

- 7.1 Subject to compliance with its obligations under Paragraph 4.1 and to the provisions of Paragraph 6, the Authority may at any time before court proceedings are commenced refer the Dispute to arbitration in accordance with the provisions of Paragraph 7.5.
- 7.2 Before the Supplier commences court proceedings or arbitration, it shall serve written notice on the Authority of its intentions and the Authority shall have 15 Working Days following receipt of such notice to serve a reply (a **“Counter Notice”**) on the Supplier requiring the Dispute to be referred to and resolved by arbitration in accordance with Paragraph 7.5 or be subject to the exclusive jurisdiction of the courts of England and Wales. The Supplier shall not commence any court proceedings or arbitration until the expiry of such 15 Working Day period.
- 7.3 If the Authority serves a Counter Notice, then:
- (a) if the Counter Notice requires the Dispute to be referred to arbitration, the provisions of Paragraph 7.5 shall apply; or
 - (b) if the Counter Notice requires the Dispute to be subject to the exclusive jurisdiction of the courts of England and Wales, the Dispute shall be so referred to those courts and the Supplier shall not commence arbitration proceedings.
- 7.4 If the Authority does not serve a Counter Notice within the 15 Working Day period referred to in Paragraph 7.2, the Supplier may either commence arbitration proceedings in accordance with Paragraph 7.5 or commence court proceedings in the Courts of England and Wales which shall (in those circumstances) have exclusive jurisdiction.
- 7.5 The Parties hereby confirm that if any arbitration proceedings are commenced pursuant to Paragraphs 7.1 to 7.4:
- (a) the Dispute shall be referred to and finally resolved by arbitration under the Rules of the London Court of International Arbitration (**“LCIA”**) (subject to Paragraphs 7.5(e), (f) and (g));
 - (b) the arbitration shall be administered by the LCIA;
 - (c) the LCIA procedural rules in force at the date that the Dispute was referred to arbitration shall be applied and are deemed to be incorporated by reference into this Contract and the decision of the arbitrator shall be binding on the Parties in the absence of any material failure to comply with such rules;
 - (d) if the Parties fail to agree the appointment of the arbitrator within 10 Working Days from the date on which arbitration proceedings are commenced or if the person appointed is unable or unwilling to act, the arbitrator shall be appointed by the LCIA;

SCHEDULE 23 (DISPUTE RESOLUTION PROCEDURE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (e) the chair of the arbitral tribunal shall be British;
- (f) the arbitration proceedings shall take place in London and in the English language;
- (g) the seat of the arbitration shall be London; and
- (h) the number of arbitrators shall be one.

8 URGENT RELIEF

8.1 Either Party may at any time take proceedings or seek remedies before any court or tribunal of competent jurisdiction:

- (a) for interim or interlocutory remedies in relation to this Contract or infringement by the other Party of that Party's Intellectual Property Rights; and/or
- (b) where compliance with Paragraph 2.1 and/or referring the Dispute to mediation may leave insufficient time for that Party to commence proceedings before the expiry of the limitation period.

9 MULTI-PARTY DISPUTES

9.1 All Multi-Party Disputes shall be resolved in accordance with the procedure set out in this Paragraph 9 (the "**Multi-Party Dispute Resolution Procedure**").

9.2 If at any time following the issue of a Dispute Notice, the Authority reasonably considers that the matters giving rise to the Dispute involve one or more Related Third Parties, then the Authority shall be entitled to determine that the Dispute is a Multi-Party Dispute and to serve a notice on the Supplier which sets out the Authority's determination that the Dispute is a Multi-Party Dispute and specifies the Related Third Parties which are to be involved in the Multi-Party Dispute Resolution Procedure, such notice a "**Multi-Party Procedure Initiation Notice**".

9.3 If following the issue of a Dispute Notice but before the Dispute has been referred to Expert Determination or to arbitration in accordance with Paragraph 7, the Supplier has reasonable grounds to believe that the matters giving rise to the Dispute have been contributed to by one or more Related Third Parties, the Supplier may serve a Supplier Request on the Authority.

9.4 The Authority shall (acting reasonably) consider each Supplier Request and shall determine within 5 Working Days whether the Dispute is:

- (a) a Multi-Party Dispute, in which case the Authority shall serve a Multi-Party Procedure Initiation Notice on the Supplier; or
- (b) not a Multi-Party Dispute, in which case the Authority shall serve written notice of such determination upon the Supplier and the Dispute shall be treated in accordance with Paragraphs 3 to 8.

SCHEDULE 23 (DISPUTE RESOLUTION PROCEDURE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 9.5 If the Authority has determined, following a Supplier Request, that a Dispute is not a Multi-Party Dispute, the Supplier may not serve another Supplier Request with reference to the same Dispute.
- 9.6 Following service of a Multi-Party Procedure Initiation Notice a Multi-Party Dispute shall be dealt with by a board (in relation to such Multi-Party Dispute, the “**Multi-Party Dispute Resolution Board**”) comprising representatives from the following parties to the Multi-Party Dispute, each of whom shall be of a suitable level of seniority to finalise any agreement with the other parties to settle the Multi-Party Dispute:
- (a) the Authority;
 - (b) the Supplier;
 - (c) each Related Third Party involved in the Multi-Party Dispute; and
 - (d) any other representatives of any of the Parties and/or any Related Third Parties whom the Authority considers necessary,
- (together “**Multi-Party Dispute Representatives**”).
- 9.7 The Parties agree that the Multi-Party Dispute Resolution Board shall seek to resolve the relevant Multi-Party Dispute in accordance with the following principles and procedures:
- (a) the Parties shall procure that their Multi-Party Dispute Representatives attend, and shall use their best endeavours to procure that the Multi-Party Dispute Representatives of each Related Third Party attend, all meetings of the Multi-Party Dispute Resolution Board in respect of the Multi-Party Dispute;
 - (b) the Multi-Party Dispute Resolution Board shall first meet within 10 Working Days of service of the relevant Multi-Party Procedure Initiation Notice at such time and place as the Parties may agree or, if the Parties do not reach agreement on the time and place within 5 Working Days of service of the relevant Multi-Party Procedure Initiation Notice, at the time and place specified by the Authority, provided such place is at a neutral location within England and that the meeting is to take place between 9.00am and 5.00pm on a Working Day; and
 - (c) in seeking to resolve or settle any Multi-Party Dispute, the members of the Multi-Party Dispute Resolution Board shall have regard to the principle that a Multi-Party Dispute should be determined based on the contractual rights and obligations between the Parties and the Related Third Parties and that any apportionment of costs should reflect the separate components of the Multi-Party Dispute.
- 9.8 If a Multi-Party Dispute is not resolved between the Parties and all Related Third Parties within 25 Working Days of the issue of the Multi-Party Procedure

SCHEDULE 23 (DISPUTE RESOLUTION PROCEDURE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Initiation Notice (or such longer period as the Parties may agree in writing), then:

- (a) either Party may serve a Mediation Notice in respect of the Multi-Party Dispute in which case Paragraph 5 shall apply;
- (b) either Party may request that the Multi-Party Dispute is referred to an expert in which case Paragraph 6 shall apply; and/or
- (c) subject to Paragraph 9.9, Paragraph 7 shall apply to the Multi-Party Dispute,

and in each case references to the "Supplier" or the "Parties" in such provisions shall include a reference to all Related Third Parties.

- 9.9 If a Multi-Party Dispute is referred to arbitration in accordance with Paragraph 7 or a Dispute becomes a Multi-Party Dispute during the course of arbitration proceedings and either Party is unable to compel a Related Third Party to submit to such arbitration proceedings, the Authority or the Supplier may discontinue such arbitration proceedings and instead initiate court proceedings. The costs of any such discontinued arbitration proceedings shall be borne by the Party which is in a direct contractual relationship with the Related Third Party or, where the Related Third Party is a Sub Contractor, by the Supplier.

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SCHEDULE 24

REPORTS AND RECORDS PROVISIONS

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 24 (*Reports and Records Provisions*)**1 TRANSPARENCY REPORTS**

- 1.1 The Parties agree that, as at the Effective Date, the Supplier shall not be required to provide any Transparency Reports (as defined in Paragraph 1.2 below). Any requirement by the Authority for the Supplier to provide any Transparency Report shall be agreed in accordance with the Change Control Procedure, following which the required Transparency Report shall be included in Annex 1 to this Schedule 24 and the remaining provisions of this Paragraph 1 shall apply,
- 1.2 Within the period agreed in the relevant Change Authorisation Note the Supplier shall provide to the Authority for its approval (such approval not to be unreasonably withheld or delayed) a draft report in accordance with Annex 1 (once approved, the “**Transparency Report(s)**”).
- 1.3 If the Authority rejects any draft Transparency Report, the Supplier shall submit a revised version of the relevant report for further approval by the Authority within five (5) days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Authority. If the Parties fail to agree on a draft Transparency Report the Authority shall determine what should be included.
- 1.4 The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Authority at the frequency referred to in Annex 1.
- 1.5 Any disagreement in connection with the preparation and/or approval of Transparency Reports, other than under Paragraph 1.3 above in relation to the contents of a Transparency Report, shall be treated as a Dispute.
- 1.6 The requirements for Transparency Reports are in addition to any other reporting requirements in this Contract.

2 OTHER REPORTS

- 2.1 The Authority may require any or all of the following reports:
- (a) delay reports;
 - (b) reports relating to Testing and tests carried out under Schedule 5 (*Security Management*) and Schedule 26 (*Service Continuity Plan and Corporate Resolution Planning*);
 - (c) reports which the Supplier is required to supply as part of the Management Information;
 - (d) annual reports on the Insurances;
 - (e) security reports; and
 - (f) Force Majeure Event reports.

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

3 RECORDS

- 3.1 The Supplier shall retain all the records (including superseded records) referred to in Annex 2 and, subject to 4.18, maintain all the records (including superseded records) referred to in Annex 3 (together "**Records**"):
- (a) in accordance with the requirements of The National Archives and Good Industry Practice;
 - (b) in chronological order;
 - (c) in a form that is capable of audit; and
 - (d) at its own expense.
- 3.2 The Supplier shall make the Records retained in accordance with Paragraph 3.1 available for inspection to the Authority on request, subject to the Authority giving reasonable notice.
- 3.3 Where Records are in electronic form, the Supplier's obligations to retain and/or maintain such Records include preserving original metadata together with all subsequent metadata in a format reasonably accessible to the Authority.
- 3.4 The Supplier shall, during the Term and a period of at least 7 years following the expiry or termination of this Contract, maintain or cause to be maintained complete and accurate documents and records in relation to the provision of the Services including but not limited to all Records.
- 3.5 Records that contain financial information shall be retained and maintained in safe storage by the Supplier for a period of at least 7 years after the expiry or termination of this Contract.
- 3.6 Without prejudice to the foregoing, the Supplier shall provide the Authority:
- (a) as soon as they are available, and in any event within 60 Working Days after the end of the first 6 months of each financial year of the Supplier during the Term, a copy, certified as a true copy by an authorised representative of the Supplier, of its un-audited interim accounts and, if applicable, of consolidated un-audited interim accounts of the Supplier and its Affiliates which would (if the Supplier were listed on the London Stock Exchange (whether or not it is)) be required to be sent to shareholders as at the end of and for each such 6 month period; and
 - (b) as soon as they shall have been sent to its shareholders in order to be laid before an annual general meeting of the Supplier, but not later than 130 Working Days after the end of each accounting reference period of the Supplier part or all of which falls during the Term, the Supplier's audited accounts and if applicable, of the consolidated audited accounts of the Supplier and its Affiliates in

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

respect of that period together with copies of all related directors' and auditors' reports and all other notices/circulars to shareholders.

4 Virtual Library

- 4.1 The Authority shall, no later than eight (8) weeks prior to the First Operational Service Commencement Date and without charge to the Supplier, host a Virtual Library on which the Supplier shall (subject to any applicable legislation governing the use or processing of personal data) make information about this Contract available in accordance with the requirements outlined in this Schedule.
- 4.2 Not used.
- 4.3 For the avoidance of doubt, the Virtual Library shall form a database which constitute Project Specific IPR which shall be assigned to the Authority pursuant to Paragraph 2.1 of Schedule 32 (*Intellectual Property Rights*) of this Contract.
- 4.4 The Supplier shall upload complete and accurate information specified in Annex 3 by the Initial Upload Date (except where prior to the launch of the Virtual Library in which case the date at which the Virtual Library is made available in accordance with Paragraph 4.1) onto Virtual Library in the format specified.
- 4.5 Except for notices under Clause 42.4 or items covered by Clause 42.6, where the Supplier is under an obligation to provide information to the Authority in a provision under this Contract, then the Supplier's upload of that information onto the Virtual Library shall satisfy the Supplier's obligation to provide the Authority with that information provided that the uploaded information meets the requirements more particularly specified in the relevant provision.
- 4.6 Except to the extent that the requirements provide for earlier and more regular Authority access to up-to-date information, Annex 3 shall not take precedence over any other obligation to provide information in this Contract and the Supplier shall refer to the applicable clause for further details as to the requirement.
- 4.7 The Supplier acknowledges that the Authority shall be entitled to provide each specified person (as set out in column 6 of the table at Annex 3) access to view and download the specified information in the Virtual Library in Annex 3 subject upon the occurrence of the event specified in the column marked Access Permission in Annex 3 to this Schedule.
- 4.8 Where Access Permission is not listed (in column 6 of the table at Annex 3) as being subject to the occurrence of a certain event the Authority may grant access to the person and information specified (in column 6 of the table at Annex 3) from the Initial Upload Date.
- 4.9 Where Access Permission is specified as being granted to the Authority's Third Party Auditor it shall:

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- (a) be entitled to access, view and download information specified in Annex 3 subject to it entering into a confidentiality agreement with the Supplier to keep the contents confidential (except to the extent disclosure of the confidential information is required under Paragraph 4.9(b) of this Schedule); and
 - (b) report to the Authority (at its request) as to the completeness and accuracy of the information but not the substance of the information.
- 4.10 The Supplier shall not do anything to prevent the Virtual Library retaining in an accessible form all historic or superseded records of the information specified Annex 3. In order to maintain the integrity of the historic archive of the information and documentation and for the purposes of maintaining a clear audit trail, the Supplier shall not delete or overwrite any information that has been stored in the Virtual Library.
- 4.11 The Supplier warrants that the information uploaded to the Virtual Library is accurate, complete, up-to-date and in accordance with this Contract at the date of upload.
- 4.12 Where the Supplier becomes aware that any of the information provided on the Virtual Library is materially inaccurate, incomplete or out of date (other than in respect of historic versions of documents) the Supplier shall provide an update to the information within fourteen (14) days unless already due to be updated beforehand due to an Update Requirement specified in Annex 3.
- 4.13 In the event of a conflict between any requirement in this Contract (excluding Annex 3) for the Supplier to provide information to the Authority and the requirements set out in Annex 3 of this Schedule, the requirement elsewhere in this Contract shall prevail.
- 4.14 Not used
- 4.15 No later than one (1) Month prior to the First Operational Services Commencement Date, the Authority shall provide training manuals to the Supplier relating to the use of the Virtual Library.
- 4.16 On request by the Supplier the Authority shall provide the Supplier's nominated users with a reasonable level of training and ongoing support to enable them to make use of the Virtual Library.
- 4.17 Not used
- 4.18 The Authority may transfer responsibility for maintaining specific Records in the Virtual Library from the Supplier to itself or to Service Recipients or to an Other Supplier, upon notifying the Supplier of the Records which the Authority will transfer such responsibility for.

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 1: TRANSPARENCY REPORTS

TITLE	CONTENT	FORMAT	FREQUENCY
N/A	N/A	N/A	N/A

There are no Transparency Reports as at the Effective Date.

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 2: RECORDS TO BE KEPT BY THE SUPPLIER

The records to be kept by the Supplier are:

- 1 This Contract, its Schedules and all amendments to such documents.
- 2 All other documents which this Contract expressly requires to be prepared.
- 3 Records relating to the appointment and succession of the Supplier Representative and each member of the Key Personnel.
- 4 Notices, reports and other documentation submitted by any Expert.
- 5 All operation and maintenance manuals prepared by the Supplier for the purpose of maintaining the provision of the Services and the underlying IT Environment and Supplier Equipment.
- 6 Documents prepared by the Supplier or received by the Supplier from a third party relating to a Force Majeure Event.
- 7 All formal notices, reports or submissions made by the Supplier to the Authority Representative in connection with the provision of the Services.
- 8 All certificates, licences, registrations or warranties in each case obtained by the Supplier in relation to the provision of the Services.
- 9 Documents prepared by the Supplier in support of claims for the Charges.
- 10 Documents submitted by the Supplier pursuant to the Change Control Procedure.
- 11 Documents submitted by the Supplier pursuant to invocation by it or the Authority of the Dispute Resolution Procedure.
- 12 Documents evidencing any change in ownership or any interest in any or all of the shares in the Supplier, where such change may cause a change of Control; and including documents detailing the identity of the persons changing such ownership or interest.
- 13 Invoices and records related to VAT sought to be recovered by the Supplier.
- 14 Financial records, including audited and un-audited accounts of the Supplier.
- 15 Records required to be retained by the Supplier by Law, including in relation to health and safety matters and health and safety files and all consents.
- 16 All documents relating to the insurances to be maintained under this Contract and any claims made in respect of them.
- 17 All journals and audit trail data referred to in Schedule 5 (*Security Management*).

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- 18 All other records, notices or certificates required to be produced and/or maintained by the Supplier pursuant to this Contract.
- 19 All records in the ITSM Toolset that are within the scope of the Supplier's responsibilities, including requirements 6.4.7.17, 6.5.2.4, 6.5.4.2 and 6.5.3.5 in Annex B (WAN Service Management Requirements) to Schedule 2 (Services Description).

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 3: RECORDS TO UPLOAD TO VIRTUAL LIBRARY

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
CI.5.5 (e), (f), 5.8(b), Paragraph 2.1(a)	Documentation	As appropriate and agreed by the Authority	Within seven (7) days of the issue of a Milestone Achievement Certificate in respect of the relevant Deliverable.	As set out for the Documentary Deliverable in the Contract or as otherwise agreed by the Authority from time to time.	Authority	Yes
CI 14.3	Key Personnel	Sch 29	Effective Date	On replacement of Key Personnel	Authority	Yes
Sch 5, Para 4.2	Core Information Management System diagram	Sch 5, Annex 3	The date specified in the Detailed Implementation Plan	Regular review and at least annually	Authority	Yes
Sch 5, Para 12.1	Security reports	As appropriate and agreed by the Authority	As requested by the Authority	Frequency and nature of which shall be as detailed and	Authority	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
				agreed in the Security Management Plan		
Sch 5, Para 8.1	IT Health Check report	As appropriate and agreed by the Authority	Prior to it submitting the Security Management Plan to the Authority for a Security Assurance Decision.	Before the Supplier is given permission by the Authority to Process or manage any Authority Data. If directed to do so by the Authority. Once every 12 months during the Term.	Authority	Yes
Sch 5, Para 7.1, 7.4, 7.6	Security certificates	Sch 5, Annex 3	Prior to receiving, storing or processing any Authority Data	-	-	No
Sch 5, Para 5	Security Management Plan	Sch 5, Annex 3	By the date specified in the Implementation	Upon update in accordance with	Authority	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
			Plan in accordance with Para 5.4 of Sch 5	Para 5 and 6 of Sch 5		
Sch 5, Para 3.3	Security Aspects Letter	Sch 5, Para 1.1	Upon signature and return of the Security Aspects Letter, in accordance with Para 3.3.2 and 3.3.3 of Sch 5 by the Supplier or any Sub-contractors that Process Authority Data	-	Authority	No
Sch 6, Para 4	Evidence of Insurances	Sch 6	Effective Date	Within fifteen (15) days after policy renewal or replacement	Authority	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
Sch 9	Commercially Sensitive Information	Sch 9	Effective Date	Upon agreement by the Authority to vary the information	Authority and/or Auditor	Yes
CI 15.7	Notified Key Subcontractors	Sch 10	Effective Date	On replacement of key subcontractor	Authority	Yes
Sch 11, Para 1	Third Party Contracts	Sch 11	Effective Date	On appointment of subcontract	Authority	Yes
CI 15.6 and 15.7	Notified Key Sub-Contractors	Sch 10	Effective Date	With each approved appointment or variation	Authority	Yes
CI 15.28	Supply chain Transparency Reports	Sch 24, Annex 4	Thirty days prior to the of the end of each financial year	Every twelve (12) months	Authority	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
CI 6.4	Detailed Implementation Plan	Sch 13	Within 20 Working Days of Effective Date	Every 3 months from Effective Date	Authority	No
CI 33.8(h)	Annual slavery and human trafficking report	As appropriate and agreed by the Authority	Within twelve (12) months	Every twelve (12) months	Authority	Yes
Sch 14, Para 4	Test Strategy	As appropriate and agreed by the Authority	Within 20 Working Days of Effective Date	Upon update to the test strategy	Authority	No
Sch 14, Para 5	Test Plan	As appropriate and agreed by the Authority	20 prior Working Days of relevant test	Upon update to the test plan	Authority	No
Sch 14, Para 8	Test Specification	As appropriate and agreed by the Authority	10 prior Working Days of relevant test	Upon update to the test specification	Authority	No
Sch 14, Para 8	Test Report	As appropriate and agreed by the Authority	2 Working Days prior to the date on which the test is planned	Reissue with each retest	Authority	No

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
			to end for the Draft Test Report 5 days for the Final Test Report following the relevant test completion			
Sch 15, Annex 4	Risk Register	Sch 15, Annex 4	Effective Date	Upon agreement by the Authority to vary the by the Risk Management Board	Authority	Yes
Sch 17, Para 4	Benchmarking Plan	Sch 17	Upon receipt from Benchmark	Approval of Plan	Authority and Auditor	Yes
Sch 17, Para 5	Benchmarking report	Sch 17	Upon receipt from Benchmark	Any update	Authority and Auditor	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
Sch 18, Para 2.3(b)	Financial Indicator Reports	Sch 18, Para 2.5	As specified in Para2.3(b) of Sch 18	As specified in Para 2.3(b) of Sch 18	Authority	Yes
Sch 18 Para 4.3(b)	Financial Distress Remediation Plan	As appropriate and agreed by the Authority	As soon as reasonably practicable and in any event within 10 Working Days of initial notification or awareness of a Financial Distress Event	On a regular basis (not less than fortnightly)	Authority	Yes
Sch 19, Part B, Para 1.1	Contract Amendment Report	Sch 19, Part B, Para 1.2	Within 1 month of a material change being agreed	-	Authority	Yes
Sch 19, Para 1.1	Quarterly Contract Report	Sch 19, Part B, Para 1.2	Within 1 month of the end of each Quarter	-	Authority	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
Sch 19, Part B, para 1.1	Annual Contract Report	Sch 19, Part B, Para 1.2	Within 1 month of the end of the Contract Year to which that report relates	-	Authority	Yes
Sch 19, Part B, para 1.1	Financial Reconciliation Report	Sch 19, Part B, Para 1.2	Within 6 months after the end of the Term	-	Authority	Yes
Sch 21, Para 3.3	Representation and Structure of boards	Sch 21 Annex 1	Within 7 days of receipt of intention, or in the case of a non-Authority board member agreement by the Authority	-	Authority	Yes
Sch 21, Para 3.5(e)	Minutes of governance meetings (all boards)	As appropriate and agreed by the Authority	Within 7 days of receipt from chairperson	-	Authority	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
Sch 22 Para 4.3	Impact Assessment Estimate	As appropriate and agreed by the Authority	Within 10 Working Days of date of receiving change request.	-	Authority	Yes
Sch 22 Para 5	Impact Assessment	As appropriate and agreed by the Authority	Within the period agreed by the Impact Assessment Estimate	Within 10 Working Days of request by the Authority to update under Schedule 22 Para 5.4	Authority	Yes
Sch 22, Para 2.6	Update full copy of the Contract and copy of annotated version illustrating changes	PDF and MS Word (editable)	Signature of Variation Date	Any variation	Authority	Yes
Sch 22, Para 4	Change Request	Sch 22, Annex 1	Within 10 Working Days of Authority issuing the Change Request	-	Authority	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
Sch 23, Para 2.1	Dispute Notice	Sch 23 Para 2.2	No longer than 20 Working Days from an unresolved dispute arising	Any variation	Authority	Yes
Sch 23, Para 2.4	Mediation Notice	As appropriate	When first served	Any variation	Authority	Yes
Sch 24, Para 1	Reports and Records Provisions	Sch 24, Annex 1	Within 3 months of the Effective Date	Frequency specified in Sch 24, Annex 1	Authority	Yes
Sch 25, Para 2.1(a)	Register of All Assets, Sub-contracts and Other Relevant Agreements	As appropriate and agreed by the Authority	Within 3 months of the Effective Date	Any variation	Authority	Yes
Sch 25, Para 2.1(b)	Configuration Database of Technical Infrastructure and	As appropriate and agreed by the Authority	Within 3 months of the Effective Date	Any variation	Authority	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
	Operating Procedures					
Sch 25, Para 3.1	Exit Information	As appropriate and agreed by the Authority	On reasonable notice given by the Authority at any point during the Term	Within 10 Working Days of Authority's written request	Authority and its potential Replacement Suppliers	Yes
Sch 25, Para 5.1	Exit Plan	Sch 25, Para 5.3	Within 3 months of the Effective Date	In the first month of each contract year; and Within 14 days if requested by the Authority following a Financial Distress Event Within 20 days after service of Termination Notice or 6 months prior to expiry of the Contract	Authority	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
Sch 25, Para 6.3(e)	Provide up to date Registers during the Termination Assistance Period	As appropriate	As requested by the Authority	As appropriate		Yes
Sch 25, Para 6.7(b)	Authority Data (handback)	Sch 25, Para 3 and/or as appropriate and agreed by the Authority	At the end of the Termination Assistance Period	-	Authority	Yes
Sch 25, Annex 1, Para 1.1, Para 1.2 Para 1.3 & Para 1.4	Termination Services supporting documentation and knowledge transfer material	As appropriate and agreed by the Authority	As specified in the Termination Assistance Notice and in any event prior to the end of the Termination Assistance Period	As specified in the Termination Assistance Notice or otherwise requested by the Authority	-	Yes
Sch 26 Service Continuity	Service Continuity Plan	Sch 26, Para 2.2	Within 40 Working Days	Sch 26, Para 7.1 and as set out in	Supplier / Authority	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
Sch 2, Annex B, requirement 6.3.3.1			from the Effective Date	Sch 2 Annex B 6.3.3.3		
Sch 26, Para 7.2	Service Continuity Plan Review Report	Sch 26, Para 6.2	Within 20 Working Days of the conclusion of each review of the Service Continuity Plan.	-	-	Yes
Sch 26, Part B	Corporate Resolution Planning Information	Sch 26, Part B, Para 2.3	Sch 26 Part B Para 2.2	Sch 26, Para 11.8	Authority	Yes
Sch 2, Annex B, requirement 6.3.4.4	Records and actions from Risk Management Board (or similar) relating to IT Service Continuity	As appropriate and agreed by the Authority	At the first monthly IT Service Continuity forum	Monthly	Authority	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
Sch 2, Annex B, requirement 6.3.4.6	ITSCM staff training record	As appropriate and agreed by the Authority	One month prior to live service commencement	Annually	Authority	Yes
Sch 2, Annex B, requirement 6.3.4.4	ITSCM single point of contact (or a designated substitute if they are unable to attend)	As appropriate and agreed by the Authority	One month prior to live service commencement	Any variation	Authority	No
Sch 18 Para 8	Board Confirmation	As set out at Annex 4 of Sch 18	Within 120 days of the first Accounting Reference Date to occur	Within 15 months of the previous Board Confirmation provided or within 120 days after each Accounting Reference Date (whichever is the earlier)	Authority	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
Sch 28, Part E, Para 1.1	Supplier's Provisional Supplier Personnel List and, Staffing Information	As appropriate and agreed by the Authority	Sch 28, Para 1.1(a) - (d)	At such intervals as are reasonably requested by the Authority	Authority	Yes
Sch 28, Part E, Para 1.2	Supplier's Final Supplier Personnel List	As appropriate and agreed by the Authority	At least 20 Working Days prior to the Service Transfer Date	Upon any material change to the list of employees	Authority and, at the discretion of the Authority, the Replacement Supplier and/or any Replacement Subcontractor	Yes
Sch 28, Part E, Para 1.6	Information relating to the manner in which the services are organised	As appropriate and agreed by the Authority	Effective Date	-	Authority	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
Sch 28, Part E, Para 1.7	Payroll and benefits information	As appropriate and agreed by the Authority	Within 5 Working Days following the Service Transfer Date	-	Authority, any Replacement Supplier and/or Replacement Sub-contractor	Yes
Sch 28, Annex E1	List of Notified Sub-contractors	As appropriate and agreed by the Authority	Effective Date	Upon any change	Authority	Yes
Sch 29	Key Personnel	Sch 29	Effective Date	As amended from time to time	Authority	Yes
Sch 31, Annex 1 Para 2.1	Reports on Data Subject Access Requests	As appropriate and agreed by the Authority	As agreed with Authority	As agreed with Authority	Authority and Supplier	Yes
Sch 2 Annex B, requirement 6.8.4.3	Device Maintenance Record	Sch 2 Annex B 6.8.4.3	As agreed with Authority	Upon completion of any maintenance	Authority	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
Sch 2 Annex B, requirement 6.3.2.5	Capacity Report	Sch 2 Annex B, requirement 6.3.2.5	At initial monthly Performance Review Board	In line with Performance Review Board	Authority and Supplier	Yes
Sch 2 Annex B, requirement 6.3.2.6	Capacity Plan	As appropriate and agreed by the Authority	As agreed with Authority	As agreed with Authority	Authority and Supplier	Yes
Sch 2 Annex B, requirement 6.3.7.7	Transition plan	As appropriate and agreed by the Authority	As agreed with Authority	As agreed with Authority	Authority and Supplier	Yes
Sch 2 Annex B, requirement 6.5.5.8	Service Improvement Plan (SIP)	As appropriate and agreed by the Authority	As agreed with Authority	As agreed with Authority	Authority and Supplier	Yes
Sch 2 Annex B, requirement 6.5.6.6	List of Supplier Personnel who require access to the ITSM Toolset and their required permission level.	As appropriate and agreed by the Authority	As agreed with Authority	Any variation	Authority	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
Sch 2 Annex B, requirement 6.7.2.2	Architecture impact assessment	As appropriate and agreed by the Authority	In accordance with the Authority's Change Management practices as described in the Processes	Any variation	Authority	Yes
Sch 32, Paragraph 6.1(c) and (d) Paragraph 6.2(c)	Licence terms for: Third Party Non-COTS Software, Third Party Non-COTS Background IPR, Third Party COTS Software Third Party COTS Background IPR	As appropriate and agreed by the Authority	Effective Date	Any variation	Authority	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
Core Terms Clause 6.1	Quality Plan	As appropriate and agreed by the Authority	Within forty (40) Working Days of the Effective Date	Upon any change	Authority and Supplier	Yes
Core Terms Clause 9.4	Maintenance Schedule	As appropriate and agreed by the Authority	As agreed with the Authority	Upon any change	Authority and Supplier	No
Sch 3 Part B, Para 1.6	Performance Monitoring Report	As set out in Para 1.6 of Part B, Sch 3	Initial Performance Review Board	Each report to be stored	Authority and Supplier	Yes
Sch 3 Part B, Para 1.7	Balanced Scorecard Report	As set out in Para 1.8 of Part B, Sch 3	Upon production in accordance with Para 1.7 of Part B, Sch 3	Each report to be stored	Authority and Supplier	Yes
Schedule 2 requirement 6.4.2.6	Knowledge Articles	As appropriate and agreed by the Authority	As agreed with Authority	Every 6 months from the initial upload of each Knowledge Article	Authority and Supplier	Yes. Each knowledge article document to be counted

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential
 Contract for the provision of WAN Services

Security Classification (Official)
 Contract reference: [REDACTED]

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)	In Scope of Knowledge Management KPI
				or as described in the ITSM Toolset		as an individual Record.
Schedule 2 requirement 7.2.1.2	Service Design Pack	As set out in the Artefact Description	Within one (1) Month of commissioning the service	In line with the Service Management requirements 6.4.2.6 to 6.4.3.1	Authority and Supplier	Yes

SCHEDULE 24 (REPORTS AND RECORDS PROVISIONS)

Confidential
 Contract for the provision of WAN Services

Security Classification (Official)
 Contract reference: [REDACTED]

ANNEX 4: SUPPLY CHAIN TRANSPARENCY INFORMATION TEMPLATE

	Financial Year 20[REDACTED]			
	Under this Contract		Supplier as a whole	
	£	%	£	%
Estimated total contract revenue (£) to be received in this Financial Year	£[REDACTED]	100%	£[REDACTED]	100%
Total value of Sub-contracted revenues (£) in this Financial Year	£[REDACTED]	[REDACTED]	£[REDACTED]	[REDACTED]
Total value of Sub-contracted revenues to SMEs (£) in this Financial Year	£[REDACTED]	[REDACTED]	£[REDACTED]	[REDACTED]
Total value of Sub-contracted revenues to VCSEs (£) in this Financial Year	£[REDACTED]	[REDACTED]	£[REDACTED]	[REDACTED]

SCHEDULE 25 (EXIT MANAGEMENT)
Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SCHEDULE 25

EXIT MANAGEMENT

Schedule 25 (*Exit Management*)

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

“Cease Impact Assessment”	has the meaning in Paragraph 11.3;
“Detailed Cease Notice”	has the meaning in Paragraph 11.6;
“Emergency Exit”	any termination of this Contract which is a: (a) termination of the whole or part of this Contract in accordance with Clause 31 (<i>Termination Rights</i>), except where the period of notice given under that Clause is greater than or equal to 6 months; (b) termination of the provision of the Services for any reason prior to the expiry of any period of notice of termination served pursuant to Clause 31 (<i>Termination Rights</i>); or (c) wrongful termination or repudiation of this Contract by either Party;
“Ethical Wall Agreement”	an ethical wall agreement in a form similar to the draft ethical wall agreement set out at Annex 2;
“Exclusive Assets”	those Assets used by the Supplier or a Key Sub-contractor which are used exclusively in the provision of the Services;
“Exit Information”	has the meaning given in Paragraph 3.1;
“Exit Manager”	the person appointed by each Party pursuant to Paragraph 2.3 for managing the Parties' respective obligations under this Schedule;
“Initial Cease Notice”	has the meaning in Paragraph 11.1;
“Initial Cease Notice Information”	has the meaning in Paragraph 11.3;

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

“Net Book Value”	the net book value of the relevant Asset(s) calculated in accordance with the depreciation policy of the Supplier set out in the letter in the agreed form from the Supplier to the Authority of the same date as this Contract;
“Non-Exclusive Assets”	those Assets (if any) which are used by the Supplier or a Key Sub-contractor in connection with the Services but which are also used by the Supplier or Key Sub-contractor for other purposes of material value;
“Ordinary Exit”	any termination of the whole or any part of this Contract which occurs: (a) pursuant to Clause 31 (<i>Termination Rights</i>) where the period of notice given by the Party serving notice to terminate pursuant to such Clause is greater than or equal to 6 months; or (b) as a result of the expiry of the Initial Term or any Extension Period;
“Transferable Assets”	those of the Exclusive Assets which are capable of legal transfer to the Authority;
“Transferable Contracts”	the Sub-contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are necessary to enable the Authority or any Replacement Supplier to perform the Services or the Replacement Services, including in relation to licences all relevant Documentation; and
“Transferring Contracts”	has the meaning given in Paragraph 7.2(c).

2 OBLIGATIONS DURING THE TERM TO FACILITATE EXIT

2.1 During the Term, the Supplier shall:

- (a) create and maintain a register of all:
 - (i) Assets, detailing their:
 - (A) make, model and asset number;

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (B) ownership and status as either Exclusive Assets or Non-Exclusive Assets;
 - (C) Net Book Value;
 - (D) condition and physical location; and
 - (E) use (including technical specifications); and
 - (ii) Sub-contracts and other relevant agreements (including relevant software and hardware licences, maintenance and support agreements, warranty support and equipment rental and lease agreements) required for the performance of the Services; and
 - (iii) other items outlined in the Exit Plan as to be described in a register;
- collectively, the “**Registers**”;
- (b) create and maintain a configuration database detailing the technical infrastructure and operating procedures, interfaces and locations through which the Supplier provides the Services, which shall contain sufficient detail to permit the Authority and/or Replacement Supplier to understand how the Supplier provides the Services and to enable the smooth transition of the Services with the minimum of disruption;
 - (c) if requested by the Authority, create and maintain, in an electronic form, user data including all active users, e-mail addresses, location and contact details (such as e-mail addresses, locations and contact details as may be advised to the Supplier by the Authority), site and software licensing information;
 - (d) agree the electronic format and access rights of the Registers with the Authority as part of the process of agreeing the Exit Plan; and
 - (e) at all times keep the Registers up to date, in particular in the event that Assets, Sub-contracts or other relevant agreements are added to or removed from the Services.
- 2.2 The Supplier shall procure that all Exclusive Assets listed in the Registers are clearly marked to identify that they are exclusively used for the provision of the Services under this Contract.
- 2.3 Each Party shall appoint a person for the purposes of managing the Parties' respective obligations under this Schedule and provide written notification of such appointment to the other Party within 3 months of the Effective Date. The Supplier's Exit Manager shall be responsible for ensuring that the Supplier and its employees, agents and Sub-contractors comply with this Schedule. The Supplier shall ensure that its Exit Manager has the requisite

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

authority to arrange and procure any resources of the Supplier as are reasonably necessary to enable the Supplier to comply with the requirements set out in this Schedule. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the termination of this Contract (in whole or in part) and all matters connected with this Schedule and each Party's compliance with it.

3 OBLIGATIONS TO ASSIST ON RE-TENDERING OF SERVICES

3.1 On reasonable notice at any point during the Term, the Supplier shall provide to the Authority and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), the following material and information in order to facilitate the preparation by the Authority of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence:

- (a) details of the Service(s);
- (b) a copy of the Registers, updated by the Supplier up to the date of delivery of such Registers;
- (c) an inventory of Authority Data in the Supplier's possession or control;
- (d) details of any third party contracts and licences, particularly any terms as regards charges, termination, assignment and novation;
- (e) a list of on-going and/or threatened disputes in relation to the provision of the Services;
- (f) to the extent permitted by applicable Law, all information relating to Transferring Supplier Employees required to be provided by the Supplier under this Contract; and
- (g) such other material and information as the Authority shall reasonably require,

(together, the "**Exit Information**").

3.2 The Supplier acknowledges that the Authority may disclose the Supplier's Confidential Information to an actual or prospective Replacement Supplier or any third party whom the Authority is considering engaging to the extent that such disclosure is necessary in connection with such engagement (except that the Authority may not under this Paragraph 3.2 disclose any Supplier's Confidential Information which is information relating to the Supplier's or its Sub-contractors' prices or costs).

3.3 The Supplier shall:

- (a) notify the Authority within 5 Working Days of any material change to the Exit Information which may adversely impact upon the potential

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

transfer and/or continuance of any Services and shall consult with the Authority regarding such proposed material changes; and

- (b) provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and in any event within 10 Working Days of a request in writing from the Authority.

3.4 The Supplier may charge the Authority for its reasonable additional costs to the extent the Authority requests more than 4 updates in any 6 month period.

3.5 The Exit Information shall be accurate and complete in all material respects and the level of detail to be provided by the Supplier shall be such as would be reasonably necessary to enable a third party to:

- (a) prepare an informed offer for those Services; and
- (b) not be disadvantaged in any subsequent procurement process compared to the Supplier (if the Supplier is invited to participate).

4 OBLIGATION TO ENTER INTO AN ETHICAL WALL AGREEMENT ON RE-TENDERING OF SERVICES

4.1 The Authority may require the Supplier to enter into the Ethical Wall Agreement at any point during a re-tendering or contemplated re-tendering of the Services or any part of the Services.

4.2 If required to enter into the Ethical Wall Agreement, the Supplier will return a signed copy of the Ethical Wall Agreement within 10 Working Days of receipt. The Supplier's costs of entering into the Ethical Wall Agreement will be borne solely by the Supplier.

5 EXIT PLAN

5.1 The Supplier shall, within 3 months after the Effective Date, deliver to the Authority an Exit Plan which:

- (a) sets out the Supplier's proposed methodology for achieving an orderly transition of the relevant Services from the Supplier to the Authority and/or its Replacement Supplier on the Partial Termination, expiry or termination of this Contract;
- (b) complies with the requirements set out in Paragraph 5.2; and
- (c) is otherwise reasonably satisfactory to the Authority.

5.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within 20 Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

5.3 The Exit Plan shall set out, as a minimum:

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (a) how the Exit Information is obtained;
- (b) separate mechanisms for dealing with Ordinary Exit and Emergency Exit, the provisions relating to Emergency Exit being prepared on the assumption that the Supplier may be unable to provide the full level of assistance which is required by the provisions relating to Ordinary Exit, and in the case of Emergency Exit, provision for the supply by the Supplier of all such reasonable assistance as the Authority shall require to enable the Authority or its sub-contractors to provide the Services;
- (c) a mechanism for dealing with Partial Termination on the assumption that the Supplier will continue to provide the remaining Services under this Contract;
- (d) the management structure to be employed during both transfer and cessation of the Services in an Ordinary Exit and an Emergency Exit;
- (e) the management structure to be employed during the Termination Assistance Period;
- (f) a detailed description of both the transfer and cessation processes, including a timetable, applicable in the case of an Ordinary Exit and an Emergency Exit;
- (g) how the Services will transfer to the Replacement Supplier and/or the Authority, including details of the processes, documentation, data transfer, systems migration, security and the segregation of the Authority's technology components from any technology components operated by the Supplier or its Sub-contractors (where applicable);
- (h) the scope of the Termination Services that may be required for the benefit of the Authority (including such of the services set out in Annex 1 as are applicable);
- (i) a timetable and critical issues for providing the Termination Services;
- (j) any charges that would be payable for the provision of the Termination Services (calculated in accordance with the methodology that would apply if such Services were being treated as a Contract Change), together with a capped estimate of such charges;
- (k) how the Termination Services would be provided (if required) during the Termination Assistance Period;

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (l) procedures to deal with requests made by the Authority and/or a Replacement Supplier for Staffing Information pursuant to Schedule 28 (*Staff Transfer*);
 - (m) include the information in the Exit Plan guidance set out in Annex 3 to this Schedule; and
 - (n) how each of the issues set out in this Schedule will be addressed to facilitate the transition of the Services from the Supplier to the Replacement Supplier and/or the Authority with the aim of ensuring that there is no disruption to or degradation of the Services during the Termination Assistance Period.
- 5.4 The Parties acknowledge that the migration of the Services from the Supplier to the Authority and/or its Replacement Supplier may be phased, such that certain of the Services are handed over before others.
- 5.5 The Supplier shall review and (if appropriate) update the Exit Plan on a basis consistent with the principles set out in this Schedule in the first month of each Contract Year (commencing with the second Contract Year) and if requested by the Authority following the occurrence of a Financial Distress Event, within 14 days of such request, to reflect any changes in the Services that have occurred since the Exit Plan was last agreed. Following such update, the Supplier shall submit the revised Exit Plan to the Authority for review. Within 20 Working Days following submission of the revised Exit Plan, the Parties shall meet and use reasonable endeavours to agree the contents of the revised Exit Plan. If the Parties are unable to agree the contents of the revised Exit Plan within that 20 Working Day period, such dispute shall be resolved in accordance with the Dispute Resolution Procedure.

Finalisation of the Exit Plan

- 5.6 Within 20 Working Days after service of a Termination Notice by either Party or 6 months prior to the expiry of this Contract, the Supplier will submit for the Authority's approval the Exit Plan in a final form that could be implemented immediately. The final form of the Exit Plan shall be prepared on a basis consistent with the principles set out in this Schedule and shall reflect any changes in the Services that have occurred since the Exit Plan was last agreed.
- 5.7 The Parties will meet and use their respective reasonable endeavours to agree the contents of the final form of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within 20 Working Days following its delivery to the Authority then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure. Until the agreement of the final form of the Exit Plan, the Supplier shall provide the Termination Services in accordance with the principles set out in this Schedule and the last approved version of the Exit Plan (insofar as relevant).

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

6 TERMINATION SERVICES**Notification of Requirements for Termination Services**

6.1 The Authority shall be entitled to require the provision of Termination Services at any time during the Term by giving written notice to the Supplier (a "**Termination Assistance Notice**") at least 4 months prior to the date of termination or expiry of this Contract or as soon as reasonably practicable (but in any event, not later than 1 month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

- (a) the date from which Termination Services are required;
- (b) the nature of the Termination Services required;
- (c) whether the Authority requires any additional services to assist with exit beyond what is required by this Schedule, which may be chargeable by the Supplier; and
- (d) the period during which it is anticipated that Termination Services and any additional services under Paragraph 6.1(c) will be required, which shall continue no longer than 24 months after the expiry of the Initial Term or any Extension Period or earlier termination of this Contract.

6.2 The Authority shall have:

- (a) an option to extend the period of assistance beyond the period specified in the Termination Assistance Notice provided that such extension shall not extend the Termination Assistance period beyond the date which is 30 months after expiry of the Initial Term or any Extension Period or earlier termination of this Contract ;and provided that it shall notify the Supplier to such effect no later than 20 Working Days prior to the date on which the provision of Termination Services is otherwise due to expire; and
- (b) the right to terminate its requirement for Termination Services by serving not less than 20 Working Days' written notice upon the Supplier to such effect.

Termination Assistance Period

6.3 Throughout the Termination Assistance Period, or such shorter period as the Authority may require, the Supplier shall:

- (a) continue to provide the Services (as applicable) and, if required by the Authority pursuant to Paragraph 6.1, provide the Termination Services;
- (b) in addition to providing the Services and the Termination Services, provide to the Authority any reasonable assistance requested by the Authority to allow the Services to continue without interruption

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

following the Partial Termination, termination or expiry of this Contract and to facilitate the orderly transfer of responsibility for and conduct of the Services to the Authority and/or its Replacement Supplier;

- (c) use all reasonable endeavours to reallocate resources to provide such assistance as is referred to in Paragraph 6.3(b) without additional costs to the Authority;
 - (d) provide the Services and the Termination Services at no detriment to the Target Performance Levels, save to the extent that the Parties agree otherwise in accordance with Paragraph 6.5; and
 - (e) at the Authority's request and on reasonable notice, deliver up-to-date Registers to the Authority.
- 6.4 Without prejudice to the Supplier's obligations under Paragraph 6.3(c), if it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.3(b) without additional costs to the Authority any additional costs incurred by the Supplier in providing such reasonable assistance which is not already in the scope of the Termination Services, the activities set out in Paragraph 1 of Annex 4 or the Exit Plan shall be subject to the Change Control Procedure.
- 6.5 If the Supplier demonstrates to the Authority's reasonable satisfaction that transition of the Services and provision of the Termination Services during the Termination Assistance Period will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Target Performance Level(s), the Parties shall vary the relevant Target Performance Level(s) and/or the applicable Service Credits to take account of such adverse effect.

Termination Obligations

- 6.6 The Supplier shall comply with all of its obligations contained in the Exit Plan in respect of any Partial Termination or termination.
- 6.7 Upon termination or expiry (as the case may be) or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Services and the Termination Services and its compliance with the other provisions of this Schedule) in respect of the Services that have been terminated, the Supplier shall:
- (a) cease to use the Authority Data;
 - (b) provide the Authority and/or the Replacement Supplier with a complete and uncorrupted version of the Authority Data in electronic form (or such other format as reasonably required by the Authority);

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (c) erase from any computers, storage devices and storage media that are to be retained by the Supplier after the end of the Termination Assistance Period all Authority Data and promptly certify to the Authority that it has completed such deletion;
 - (d) return to the Authority such of the following as is in the Supplier's possession or control:
 - (i) all copies of the Authority Software and any other software licensed by the Authority to the Supplier under this Contract;
 - (ii) all materials created by the Supplier under this Contract in which the IPRs are owned by the Authority;
 - (iii) any parts of the IT Environment and any other equipment which belongs to the Authority; and
 - (iv) any items that have been on-charged to the Authority, such as consumables;
 - (e) vacate any Authority Premises unless access is required to continue to deliver the Services;
 - (f) provide access during normal working hours to the Authority and/or the Replacement Supplier for up to 12 months after the Partial Termination, expiry or termination of this Contract to:
 - (i) such information relating to the Services as remains in the possession or control of the Supplier; and
 - (ii) such members of the Supplier Personnel as have been involved in the design, development and provision of the Services and who are still employed by the Supplier, provided that the Authority and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to requests for access under this Paragraph 6.7(f)(ii).
- 6.8 Upon Partial Termination, termination or expiry (as the case may be) or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Services and the Termination Services and its compliance with the other provisions of this Schedule), each Party shall return to the other Party (or if requested, destroy or delete) all Confidential Information of the other Party in respect of the terminated Services and shall certify that it does not retain the other Party's Confidential Information save to the extent (and for the limited period) that such information needs to be retained by the Party in question for the purposes of providing or receiving any Services or Termination Services or for statutory compliance purposes.

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 6.9 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Authority to the Supplier in relation to the terminated Services shall be terminated with effect from the end of the Termination Assistance Period.

7 ASSETS, SUB-CONTRACTS AND SOFTWARE

- 7.1 Following notice of termination or Partial Termination of this Contract and during the Termination Assistance Period, the Supplier shall not, in respect of the terminated Services, without the Authority's prior written consent:

- (a) terminate, enter into or vary any Sub-contract except to the extent that such change does not or will not affect the provision of Services or the Charges;
- (b) (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Assets or acquire any new Assets; or
- (c) terminate, enter into or vary any licence for software in connection with the Services.

- 7.2 Within 20 Working Days of receipt of the up-to-date Registers provided by the Supplier pursuant to Paragraph 6.3(e), the Authority shall provide written notice to the Supplier setting out:

- (a) which, if any, of the Transferable Assets the Authority requires to be transferred to the Authority and/or the Replacement Supplier in respect of the terminated Services ("**Transferring Assets**");
- (b) which, if any, of:
 - (i) the Exclusive Assets that are not Transferable Assets; and
 - (ii) the Non-Exclusive Assets,the Authority and/or the Replacement Supplier requires the continued use of; and
- (c) which, if any, of Transferable Contracts the Authority requires to be assigned or novated to the Authority and/or the Replacement Supplier (the "**Transferring Contracts**"),

in order for the Authority and/or its Replacement Supplier to provide the Services from the expiry of the Termination Assistance Period. Where requested by the Authority and/or its Replacement Supplier, the Supplier shall provide all reasonable assistance to the Authority and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts the Authority and/or its Replacement Supplier requires to provide the Services or Replacement Services. Where requested by the Supplier, the Authority and/or its Replacement Supplier shall discuss in good faith with the

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Supplier which Transferable Contracts are used by the Supplier in matters unconnected to the Services or Replacement Services.

- 7.3 With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Authority and/or its nominated Replacement Supplier for a consideration equal to their Net Book Value, except where:
- (a) a Termination Payment is payable by the Authority to the Supplier, in which case, payment for such Assets shall be included within the Termination Payment; or
 - (b) the cost of the Transferring Asset has been partially or fully paid for through the Charges at the time of expiry or termination of this Contract, in which case the Authority shall pay the Supplier the Net Book Value of the Transferring Asset less the amount already paid through the Charges.
- 7.4 Risk in the Transferring Assets shall pass to the Authority or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title to the Transferring Assets shall pass to the Authority or the Replacement Supplier (as appropriate) on payment for the same.
- 7.5 Where the Supplier is notified in accordance with Paragraph 7.2(c) that the Authority and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:
- (a) procure a non-exclusive, perpetual, royalty-free licence (or licence on such other terms that have been agreed by the Authority) for the Authority and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which
 - (b) procure a suitable alternative to such assets and the Authority or the Replacement Supplier shall bear the reasonable proven costs of procuring the same.
- 7.6 The Supplier shall as soon as reasonably practicable assign or procure the novation to the Authority and/or the Replacement Supplier of the Transferring Contracts. The Supplier shall execute such documents and provide such other assistance as the Authority reasonably requires to effect this novation or assignment.
- 7.7 The Authority shall:
- (a) accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and
 - (b) once a Transferring Contract is novated or assigned to the Authority and/or the Replacement Supplier, carry out, perform and discharge

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.

- 7.8 The Supplier shall hold any Transferring Contracts on trust for the Authority until such time as the transfer of the relevant Transferring Contract to the Authority and/or the Replacement Supplier has been effected.
- 7.9 The Supplier shall indemnify the Authority (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Authority (and/or Replacement Supplier) pursuant to Paragraph 7.6 both:
- (a) in relation to any matters arising prior to the date of assignment or novation of such Sub-contract; and
 - (b) in relation to any matters arising after the date of assignment or novation of such Sub-contract where the loss, liability or cost arises as a result of the Supplier's failure to comply with Clause 16 (*Intellectual Property Rights*) and/or Schedule 32 (*Intellectual Property Rights*).

8 SUPPLIER PERSONNEL

- 8.1 The Authority and Supplier agree and acknowledge that in the event of the Supplier ceasing to provide the Services or part of them for any reason, Schedule 28 (*Staff Transfer*) shall apply.
- 8.2 The Supplier shall not take any step (expressly or implicitly or directly or indirectly by itself or through any other person) to dissuade or discourage any employees engaged in the provision of the Services from transferring their employment to the Authority and/or the Replacement Supplier.
- 8.3 During the Termination Assistance Period, the Supplier shall give the Authority and/or the Replacement Supplier reasonable access to the Supplier's personnel to present the case for transferring their employment to the Authority and/or the Replacement Supplier.
- 8.4 The Supplier shall immediately notify the Authority or, at the direction of the Authority, the Replacement Supplier of any period of notice given by the Supplier or received from any person referred to in the Staffing Information, regardless of when such notice takes effect.
- 8.5 The Supplier shall not for a period of 12 months from the date of transfer re-employ or re-engage or entice any employees, suppliers or Sub-contractors whose employment or engagement is transferred to the Authority and/or the Replacement Supplier, except that this Paragraph shall not apply where the employee, supplier or Sub-contractor applies in response to a public advertisement of a vacancy.

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

9 CHARGES

- 9.1 During the Termination Assistance Period (or for such shorter period as the Authority may require the Supplier to provide the Termination Services), the Authority shall pay the Charges to the Supplier in respect of the Termination Services in accordance with the rates set out in the Exit Plan (but shall not be required to pay costs in excess of the estimate set out in the Exit Plan). If the scope or timing of the Termination Services is changed and this results in a change to the costs of such Termination Services, the estimate may be varied in accordance with the Change Control Procedure.
- 9.2 Not used.
- 9.3 For the purpose of calculating the costs of providing the Termination Services for inclusion in the Exit Plan or, if no Exit Plan has been agreed, the costs of providing Termination Services shall be determined in accordance with the Change Control Procedure.
- 9.4 Except as otherwise expressly specified in this Contract, the Supplier shall not make any charges for the services provided by the Supplier pursuant to, and the Authority shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with, this Schedule including the preparation and implementation of the Exit Plan, the activities set out in Paragraph 1 of Annex 4 and any other activities mutually agreed between the Parties to carry on after the expiry of the Termination Assistance Period.

10 APPORTIONMENTS

- 10.1 All outgoings and expenses (including any remuneration due) and all rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Authority and the Supplier and/or the Replacement Supplier and the Supplier (as applicable) as follows:
- (a) the amounts shall be annualised and divided by 365 to reach a daily rate;
 - (b) the Authority shall be responsible for (or shall procure that the Replacement Supplier shall be responsible for) or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and
 - (c) the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.
- 10.2 Each Party shall pay (and/or the Authority shall procure that the Replacement Supplier shall pay) any monies due under Paragraph 10.1 as soon as reasonably practicable.

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

11 PARTIAL TERMINATION FOR CONVENIENCE OF SERVICES

11.1 If the Authority elects to partially terminate for convenience any part of the Services in accordance with Clause 31.1A (Partial Termination for Convenience), the Authority shall provide written notification (the “**Initial Cease Notice**”) to the Supplier that it intends to terminate part of the Services. The Initial Cease Notice shall follow the structure of the Change Request (as defined in Part A (Change Control Procedure) of Schedule 22 (Change Control Procedure, Service Requests and Projects) and shall include:

- 11.1.1 a description of the part of the Services to be terminated;
- 11.1.2 the Termination Assistance, if required and known by the Authority at this stage;
- 11.1.3 the forecast date(s) on which the Services are forecast to begin to cease and terminate completely;
- 11.1.4 the estimated impact on the Charges with reference to the Charges that will cease, and the estimated new monthly Charges;
- 11.1.5 the party or parties that will be carrying out the Replacement Services which for the avoidance of doubt may include the Authority; and
- 11.1.6 any other relevant information that either Party deems necessary to be included in such notice,

provided always that the Initial Cease Notice shall be served by the Authority to the Supplier at least three (3) months’ in advance of the start of the period in Paragraph 11.1.3.

11.2 As soon as is reasonably practicable following service of an Initial Cease Notice the Supplier may request a meeting or meetings (either in person or online) with the Authority to discuss the contents of the Initial Cease Notice. The Parties shall use reasonable endeavours to hold any such meeting within five (5) Working Days of service of the Initial Cease Notice.

11.3 The Supplier shall, acting in good faith, complete and submit to the Authority in writing, within twenty (20) Working Days (or such other period as may be agreed between the Parties) of receipt of an Initial Cease Notice from the Authority, an assessment of the Initial Cease Notice (a “**Cease Impact Assessment**”) which shall contain:

- 11.3.1 details of the Services identified in the Initial Cease Notice;
- 11.3.2 details of Termination Assistance, if applicable;
- 11.3.3 recommendations on an appropriate timescale for the Termination Assistance Period which the Authority may take into account or ignore at its sole discretion;

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 11.3.4 details of the impact of terminating the Services detailed in the Initial Cease Notice on the remaining Services and the Supplier's ability to meet its obligations under the remaining parts of the Contract;
 - 11.3.5 details of the impact on any work in progress that may also be affected by the termination of the Services;
 - 11.3.6 particulars of any changes which would be required to the Exit Plan in order to terminate the Services by the forecast date(s);
 - 11.3.7 particulars of the other changes (if any) which would be required to the Contract and to be implemented using the Change Control Procedure, in order to terminate the Services;
 - 11.3.8 a detailed breakdown and such supporting evidence of the costs and resources reasonably required to successfully cease the Services by the forecast date(s);
 - 11.3.9 the full cost and risk implications for the Authority that would result from terminating the Services including whether any Annual Shortfall Amount (as defined in Schedule 15 (*Charges and Invoicing*)) is payable; and
 - 11.3.10 such other information as the Authority may reasonably request in the Initial Cease Notice,
- together, the **"Initial Cease Notice Information"**.
- 11.4 Within twenty (20) Working Days (or such other period as agreed by the Parties in writing) of receiving the Cease Impact Assessment, the Authority shall evaluate the Cease Impact Assessment and the Initial Cease Notice Information and shall do one of the following:
- 11.4.1 approve the Cease Impact Assessment, in which case the Parties shall continue to work together with respect to the forecast date(s) to terminate the Services, and any changes that may be required to the Contract or Exit Plan; or
 - 11.4.2 in its absolute discretion reject the Cease Impact Assessment, in which case it shall notify the Supplier in writing of the rejection with reasons; or
 - 11.4.3 in the event that it reasonably believes that the Supplier has not complied with the requirements of Paragraph 11.3 or the Initial Cease Notice Information contains errors or omissions and/or further information is required to properly evaluate the Cease Impact Assessment, require the Supplier to make such modifications accordingly and/or supply the further information requested and resubmit the same to the Authority within five (5)

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Working Days of the Authority's request (or such other period as may be agreed by the Parties in writing); or

- 11.4.4 approve the Cease Impact Assessment on a conditional basis if in the Authority's opinion the Cease Impact Assessment contains errors or omissions and/or further information is required but that this should not delay proceeding with the termination of the relevant Services. If the Cease Impact Assessment is approved on a conditional basis, the Authority shall provide the Supplier with details of errors, omissions and/or further information required and the associated timescales, acting reasonably.
- 11.5 If the Authority approves the Cease Impact Assessment pursuant to Paragraphs 11.4.1 or 11.4.4 above, then it shall inform the Supplier and unless it is agreed by both Parties that a detailed Exit Plan is not required for the Services, the Supplier shall prepare and submit to the Authority within twenty (20) Working Days (or such other period as may be agreed between the Parties taking account of the nature and complexity of the requirements) of receipt of the Authority's notice of approval, a detailed Exit Plan in relation to the Services which are to be terminated and reflecting all relevant details from the approved Cease Impact Assessment, including the following:
 - 11.5.1 the Supplier's suggested approach to terminating the relevant Services based on the Supplier's knowledge and expertise;
 - 11.5.2 indicative cost estimates, applicable to the relevant Services;
 - 11.5.3 how the Services will transfer to the Replacement Supplier, including details of the processes, documentation, data migration and transfer, asset transfer, systems migration, software, security, third party contracts and licences and the segregation of the Authority's technology components from any technology components operated by the Supplier or its Sub-Contractors (where applicable);
 - 11.5.4 a timetable and critical issues for providing any Termination Assistance;
 - 11.5.5 any charges that would be payable for the provision of the Termination Assistance, together with an indicative estimate of such charges supported in each case by particulars of the estimate.
- 11.6 Once the Authority has sufficient certainty in relation to the date that the relevant Services will terminate, having regard to the likely dates that the Replacement Services will be ready, the Authority shall promptly issue a written notice to the Supplier (the "**Detailed Cease Notice**"). The Detailed Cease Notice shall be in line with the approved Cease Impact Assessment and confirm:
 - 11.6.1 the Services to be terminated;

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 11.6.2 any Termination Assistance that the Authority requires;
 - 11.6.3 the date(s) on which the Services will terminate;
 - 11.6.4 the impact on the Charges with reference to the Charges that will cease from the date the Services terminate, and the new Charges in accordance with the provisions of Paragraph 4.3.5 (Minimum Circuit Charges) of Part A (Pricing) of Schedule 15 (*Charges and Invoicing*) and the principles set out in Schedule 16 (Payments on Termination), provided always that no Compensation Payment shall be payable by the Authority in accordance with paragraph 6.4 of Schedule 16 (Payments on Termination);
 - 11.6.5 the party or parties that will be carrying out the Replacement Services; and
 - 11.6.6 any relevant or associated information that the Authority deems necessary to include in such a notice,
- provided always that the Detailed Cease Notice shall be served by the Authority to the Supplier at least one (1) calendar month in advance of the date of termination of the Services.
- 11.7 The Supplier acknowledges that the Authority is reliant upon the Replacement Services being ready and therefore for the avoidance of doubt the forecast date for the Services to terminate as provided for in the Initial Cease Notice may differ to the date set out in the Detailed Cease Notice.
 - 11.8 Until such time as the Authority issues a Detailed Cease Notice, the Supplier shall continue to provide the remaining Services to the end of the Term in accordance with the Contract.
 - 11.9 Without prejudice to any other rights and remedies of the Authority howsoever arising, any Default by the Supplier in its performance of its obligations under this Paragraph 11 that has or is likely to have a material adverse effect on the Authority's ability to operate the partial termination processes in this Paragraph 11 may be treated by the Authority as a material Default for the purposes of Clause 25.1(c).
 - 11.10 Any disputes arising out of this Schedule shall be dealt with in accordance with Schedule 23 (Dispute Resolution Procedure).
 - 11.11 A diagram summarising the key steps and notices required in the partial termination process described in this Paragraph 11, is set out in Annex 5 below. The diagram is for illustration purposes only.

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 1: SCOPE OF THE TERMINATION SERVICES

- 1.1 The Termination Services to be provided by the Supplier shall include such of the following services as the Authority may specify:
- (a) ceasing all non-critical Software changes (except where agreed in writing with the Authority);
 - (b) notifying the Sub-contractors of procedures to be followed during the Termination Assistance Period and providing management to ensure these procedures are followed;
 - (c) providing assistance and expertise as necessary to examine all operational and business processes (including all supporting documentation) in place and re-writing and implementing processes and procedures such that they are appropriate for use by the Authority and/or the Replacement Supplier after the end of the Termination Assistance Period;
 - (d) delivering to the Authority the existing systems support profiles, monitoring or system logs, problem tracking/resolution documentation and status reports all relating to the 12 month period immediately prior to the commencement of the Termination Services;
 - (e) providing details of work volumes and staffing requirements over the 12 month period immediately prior to the commencement of the Termination Services;
 - (f) with respect to work in progress as at the end of the Termination Assistance Period or such other date as may be required by the Authority, (i) providing a list of work in progress which includes as a minimum a description of each item of work in progress, documenting the current status and (ii) stabilising for continuity during transition;
 - (g) providing the Authority with any problem logs which have not previously been provided to the Authority;
 - (h) providing assistance and expertise as necessary to examine all governance and reports in place for the provision of the Services and re-writing and implementing these during and for a period of 12 months after the Termination Assistance Period;
 - (i) providing assistance and expertise as necessary to examine all relevant roles and responsibilities in place for the provision of the Services and re-writing and implementing these such that they are appropriate for the continuation of the Services after the Termination Assistance Period;

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (j) agreeing with the Authority an effective communication strategy and joint communications plan which sets out the implications for Supplier Personnel, Authority staff, customers and key stakeholders;
- (k) reviewing all Software libraries used in connection with the Services and providing details of these to the Authority and/or the Replacement Supplier;
- (l) providing assistance and expertise as necessary to support the Authority and/or the Replacement Supplier develop the migration plan for business operations and Authority Data to the Replacement Supplier, which may include migration approach, testing of plans, contingency options, and handling of historic or archived Authority Data;
- (m) provide all necessary support, equipment, tools, and Software such as data migration services and/or Automated Programming Interfaces, in order to enable and support the execution of the migration plan by the Authority and/or Replacement Supplier;
- (n) making available to the Authority and/or the Replacement Supplier expertise to analyse training requirements and provide all necessary training for the use of tools by such staff as are nominated by the Authority (acting reasonably) at the time of termination or expiry;
- (o) assisting in establishing naming conventions for any new production site;
- (p) analysing and providing information about capacity and performance requirements, processor requirements and bandwidth requirements, and known planned requirements for capacity growth across these areas;
- (q) generating a computer listing of the Source Code of such Supplier Software as the Authority may request, in a form and on media reasonably requested by the Authority. It is acknowledged by the Parties that as at the Effective Date no Supplier Software is being used in the delivery of the Services;
- (r) agreeing with the Authority a handover plan for all of the Supplier's responsibilities as set out in the Security Management Plan;
- (s) delivering copies of the production databases (with content listings) to the Authority's and/or the Replacement Supplier's operations staff (on appropriate media) as reasonably requested by the Authority;
- (t) assisting with the loading, testing and implementation of the production databases;

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (u) assisting in the execution of a parallel operation until the effective date of expiry or termination of this Contract;
- (v) in respect of the maintenance and support of the Supplier System, providing historical performance data for the previous twenty-four (24) months ;
- (w) assisting in the execution of a parallel operation of the maintenance and support of the Supplier System until the end of the Termination Assistance Period or as otherwise specified by the Authority (provided that these Services shall end on a date no later than the end of the Termination Assistance Period);
- (x) providing an information pack listing and describing the Services for use by the Authority in the procurement of the Replacement Services;
- (y) answering all reasonable questions from the Authority and/or the Replacement Supplier regarding the Services;
- (z) agreeing with the Authority and/or the Replacement Supplier a plan for the migration of the Authority Data to the Authority and/or the Replacement Supplier;
- (aa) providing access to the Authority and/or the Replacement Supplier during the Termination Assistance Period and for a period not exceeding 6 months afterwards for the purpose of the smooth transfer of the Services to the Authority and/or the Replacement Supplier:
 - (i) to information and documentation relating to the Transferring Services that is in the possession or control of the Supplier or its Sub-contractors (and the Supplier agrees and shall procure that its Sub-contractors do not destroy or dispose of that information within this period) including the right to take reasonable copies of that material; and
 - (ii) following reasonable notice and during the Supplier's normal business hours, to members of the Supplier Personnel who have been involved in the provision or management of the Services and who are still employed or engaged by the Supplier or its Sub-contractors; and
- (bb) knowledge transfer services, including:
 - (i) transferring all training material and providing appropriate training to those Authority and/or Replacement Supplier staff responsible for internal training in connection with the provision of the Services;

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (ii) providing for transfer to the Authority and/or the Replacement Supplier of all knowledge reasonably required for the provision of the Services which may, as appropriate, include information, records and documents;
- (iii) providing the Supplier and/or the Replacement Supplier with access to such members of the Supplier's or its Sub-contractors' personnel as have been involved in the design, development, provision or management of the Services and who are still employed or engaged by the Supplier or its Sub-contractors; and
- (iv) allowing the Authority and/or the Replacement Supplier to work alongside and observe the performance of the Services by the Supplier at its Sites used to fulfil the Services (subject to compliance by the Authority and the Replacement Supplier with any applicable security and/or health and safety restrictions,

and any such person who is provided with such knowledge transfer services will sign a confidentiality undertaking in favour of the Supplier (in such form as the Supplier shall reasonably require)).

1.2 The Supplier shall:

- (a) provide a documented plan relating to the training matters referred to in Paragraph 1.1(n) for agreement by the Authority at the time of termination or expiry of this Contract;
- (b) co-operate fully in the execution of the handover plan agreed pursuant to Paragraph 1.1(r), providing skills and expertise of a suitable standard; and
- (c) fully co-operate in the execution of the Authority Data migration plan agreed pursuant to Paragraph 1.1(z), providing skills and expertise of a reasonably acceptable standard.

1.3 To facilitate the transfer of knowledge from the Supplier to the Authority and/or its Replacement Supplier, the Supplier shall provide a detailed explanation of the procedures and operations used to provide the Services, the change management process and other standards and procedures to the operations personnel of the Authority and/or the Replacement Supplier.**1.4 The information which the Supplier shall provide to the Authority and/or the Replacement Supplier pursuant to Paragraph 1.1(aa) 1.1(z) shall include:**

- (a) copies of up-to-date procedures and operations manuals;
- (b) product information;

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (c) agreements with third party suppliers of goods and services which are to be transferred to the Authority and/or the Replacement Supplier;
- (d) key support contact details for third party supplier personnel under contracts which are to be assigned or novated to the Authority pursuant to this Schedule;
- (e) information regarding any unresolved faults in progress at the commencement of the Termination Assistance Period as well as those expected to be in progress at the end of the Termination Assistance Period;
- (f) details of physical and logical security processes and tools which will be available to the Authority; and
- (g) any relevant interface information,

and such information shall be updated by the Supplier at the end of the Termination Assistance Period.

1.5 During the Termination Assistance Period the Supplier shall grant any agent or personnel (including employees, consultants and Suppliers) of the Replacement Supplier and/or the Authority access, during business hours and upon reasonable prior written notice, to any Sites for the purpose of effecting a prompt knowledge transfer provided that:

- (a) any such agent or personnel (including employees, consultants and suppliers) having access to any Sites pursuant to this Paragraph 1.5 shall:
 - (i) sign a confidentiality undertaking in favour of the Supplier (in such form as the Supplier shall reasonably require); and
 - (ii) during each period of access comply with the security, systems and facilities operating procedures of the Supplier relevant to such Site and that the Authority deems reasonable; and
- (b) the Authority and/or the Replacement Supplier shall pay the reasonable, proven and proper costs of the Supplier incurred in facilitating such access.

SCHEDULE 25 (EXIT MANAGEMENT)
Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 2: DRAFT ETHICAL WALL AGREEMENT

[THE AUTHORITY]

and

[THE COUNTERPARTY]

ETHICAL WALL AGREEMENT

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

This Agreement is dated [REDACTED] 20[REDACTED] (the "Effective Date").

Between:

- (1) [INSERT NAME OF AUTHORITY] (the "**Authority**") [acting on behalf of the Crown] of [insert Authority's address]; and
- (2) [NAME OF COUNTERPARTY] a [company]/[limited liability partnership] registered in England and Wales under registered number [insert registered number] whose registered office is at [insert Counterparty's registered address] (the "**Counterparty**"),

together the "**Parties**" and each a "**Party**".

BACKGROUND

- A. The Authority is obliged to ensure transparency, fairness, non-discrimination and equal treatment in relation to its procurement process pursuant to the Procurement Regulations (defined below). The purpose of this document ("**Agreement**") is to define the protocols to be followed to prevent, identify and remedy any conflict of interest (whether actual, potential or perceived) in the context of the Purpose (defined below).
- B. The Authority is conducting a procurement exercise for the [supply/purchase/provision] of [insert details of project/goods/services] (the "**Purpose**").
- C. The Parties wish to enter into this Agreement to ensure that a set of management processes, barriers and disciplines are put in place to ensure that conflicts of interest do not arise, and that the Counterparty does not obtain an unfair competitive advantage over Other Bidders.

IT IS AGREED:**1 DEFINITIONS AND INTERPRETATION**

- 1.1 The following capitalised words and expressions shall have the following meanings in this Agreement and its recitals:

"**Affiliate**" means in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;

"**Agreement**" means this ethical walls agreement duly executed by the Parties;

"**Bid Team**" means any Representatives of the Counterparty, any of its Affiliates and/or any Subcontractors connected to the preparation of an ITT Response;

"**Central Government Body**" means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Classification Guide, as published and amended from time to time by the Office for National Statistics, including:

- a) Government Departments;
- b) Non-Departmental Public Bodies or Assembly Sponsored Public Bodies (advisory, executive, or tribunal);
- c) Non-Ministerial Departments; or
- d) Executive Agencies;

"Conflicted Personnel" means any Representatives of:

- a) the Counterparty;
- b) any of the Counterparty's Affiliates; and/or
- c) any Subcontractors,

who, because of the Counterparty's, any of its Affiliates' and/or any Subcontractors' relationship with the Authority under any Contract, have or have had access to information which creates or may create a conflict of interest or provide the Bid Team with an unfair advantage as regards information Other Bidders would not have;

"Contract" means any pre-existing or previous contract between the Authority and:

- (a) the Counterparty;
- (b) any of the Counterparty's Affiliates;
- (c) any Subcontractor; and
- (d) any other Third Party,

relating to the subject matter of the Purpose at the date of the commencement of the ITT Process;

"Control" means the beneficial ownership of more than 50% of the issued share capital of a company or the legal power to direct or cause the direction of the management of the company and **"Controls"** and **"Controlled"** shall be interpreted accordingly;

"Effective Date" means the date of this Agreement as set out above;

"Invitation to Tender" or **"ITT"** means an invitation to submit tenders issued by the Authority as part of an ITT Process (and shall include an Invitation to Negotiate);

"ITT Process" means, with regard to the Purpose, the relevant procedure provided for in the Procurement Regulations (as amended), which the Authority has elected to use to select a contractor or contractors, together with all relevant information, data, correspondence and/or documents issued and/or made available by or on behalf of the Authority as part of that procurement exercise and all information, correspondence and/or documents issued and/or made

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

available by or on behalf of the bidders in response together with any resulting contracts;

"ITT Response" means the tender(s) submitted, or to be submitted, by the Counterparty, any of its Affiliates and/or any Subcontractors in response to any invitation(s) to submit bids under the ITT process;

"Other Bidder" means any other bidder or potential bidder that is not the Counterparty or any of its Affiliates that has taken or is taking part in the ITT Process;

"Procurement Process" means the period commencing on the earlier of: (a) the publication of the first notice in relation to the Purpose; and (b) the execution of this Agreement, and ending on the occurrence of: (i) the publication by the Authority of all contract award notices that result from the ITT Process; or (ii) the abandonment or termination of the ITT Process as notified by the Authority;

"Procurement Regulations" means the Public Contracts Regulations 2015, the Public Procurement (Amendment etc.)(EU Exit) Regulations 2020, the Defence and Security Public Contracts Regulations 2011, the Utilities Contracts Regulations 2016, and the Concession Contracts Regulations 2016, each as amended from time to time;

"Professional Advisor" means a supplier, subcontractor, advisor or consultant engaged by the Counterparty and/or any of its Affiliates under the auspices of compiling its ITT response;

"Purpose" has the meaning given to it in recital B to this Agreement;

"Representative" refers to a person's officers, directors, employees, advisers (including the officers, directors, employees, advisers and agents of any Professional Advisors), agents and, where the context admits, providers or potential providers of finance (including their representatives) to the Counterparty, any of its Affiliates and/or any subcontractors engaged in connection with the ITT Process;

"Subcontractor" means an existing or proposed subcontractor of:

- a) the Counterparty; and/or
- b) any of the Counterparty's Affiliates,

who is connected to the preparation of an ITT Response (including key subcontractors named in the ITT Response);

"Third Party" means any person who is not a Party, including Other Bidders, their Affiliates and/or their Representatives; and

"Working Day" means any day of the week other than a weekend, when Banks in England and Wales are open for business.

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 1.2 Reference to the disclosure of information includes any communication or making available information and includes both direct and indirect disclosure.
- 1.3 Reference to the disclosure of information, or provision of access, by or to the Authority, the Counterparty, any of the Counterparty's Affiliates and/or any Subcontractors includes disclosure, or provision of access, by or to the Representatives of the Authority, the Counterparty, any of its Affiliates and/or any Subcontractors (as the case may be).
- 1.4 Reference to persons includes legal and natural persons.
- 1.5 Reference to any enactment is to that enactment as amended, supplemented, re-enacted or replaced from time to time.
- 1.6 Reference to clauses and recitals is to clauses of and recitals to this Agreement.
- 1.7 Reference to any gender includes any other.
- 1.8 Reference to writing includes email.
- 1.9 The terms "**associate**", "**holding company**", "**subsidiary**", "**subsidiary undertaking**" and "**wholly owned subsidiary**" have the meanings attributed to them in the Companies Act 2006, except that for the purposes of section 1159(1)(a) of that Act, the words 'holds a majority of the voting rights' shall be changed to 'holds 30% or more of the voting rights', and other expressions shall be construed accordingly.
- 1.10 The words "**include**" and "**including**" are to be construed without limitation.
- 1.11 The singular includes the plural and vice versa.
- 1.12 The headings contained in this Agreement shall not affect its construction or interpretation.

2 ETHICAL WALLS

- 2.1 In consideration of the sum of £1 payable by the Authority to the Counterparty, receipt of which is hereby acknowledged, the Parties agree to be bound by the terms of this Agreement.

Conflicts of Interest

- 2.2 The Counterparty:
- 2.2.1 shall take all appropriate steps to ensure that neither the Counterparty, nor its Affiliates, nor any Subcontractors nor any Representatives are in a position where, in the reasonable opinion of the Authority, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Counterparty, any of its Affiliates, any Subcontractors and/or any Representatives and the duties owed to the

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Authority under any Contract or pursuant to an open and transparent ITT Process; and

- 2.2.2 acknowledges and agrees that a conflict of interest may arise in situations where the Counterparty, any of its Affiliates, any Subcontractors and/or any Representatives intend to take part in the ITT Process and because of the Counterparty's, any of its Affiliates', any Subcontractors' and/or any Representatives' relationship with the Authority under any Contract, the Counterparty, any of its Affiliates, any Subcontractors and/or any Representatives have or have had access to information which could provide the Counterparty, any of its Affiliates, any Subcontractors and/or any Representatives with an advantage and render unfair an otherwise genuine and open competitive ITT Process.
- 2.3 Where there is or is likely to be a conflict of interest, or the perception of a conflict of interest, of any kind in relation to the ITT Process, the Counterparty shall take such steps that are necessary to eliminate the conflict of interest to the Authority's satisfaction, including one or more of the following:
- 2.3.1 not assigning any of the Conflicted Personnel to the Bid Team at any time;
- 2.3.2 providing to the Authority promptly upon request a complete and up to date list of any Conflicted Personnel and the personnel comprising the Bid Team and reissue such list to the Authority promptly upon any change to it;
- 2.3.3 ensuring that no act or omission by itself, its Affiliates, any Subcontractors and/or any Representatives results in information of any kind, however conveyed, or in any format and however so stored:
- (a) about the ITT Process (gleaned from the performance of any Contract or otherwise); and/or
 - (b) which would or could in the opinion of the Authority confer an unfair advantage on the Counterparty in relation to its participation in the ITT Process,
- becoming available to the Bid Team where the Authority has not made generally available that information to Other Bidders;
- 2.3.4 ensuring that by no act or omission by itself, its Affiliates, any Subcontractors and/or any Representatives and in particular the Bid Team results in information of any kind, however conveyed, in any format and however so stored about the ITT Process, its operation and all matters connected or ancillary to it becoming available to the Conflicted Personnel;

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 2.3.5 ensure that agreements that flow down the Counterparty's obligations in this Agreement, are entered into as necessary, between the Counterparty and its Affiliates and any Subcontractors [in a form to be approved by the Authority];
- 2.3.6 physically separating the Conflicted Personnel and the Bid Team, either in separate buildings or in areas with restricted access;
- 2.3.7 providing regular training to its Affiliates, any Subcontractors and/or Representatives to ensure it is complying with this Agreement;
- 2.3.8 monitoring Conflicted Personnel movements within restricted areas (both physical and electronic online areas) to ensure it is complying with this Agreement and to ensure adherence to the ethical wall arrangements the Counterparty, its Affiliates, any Subcontractors and/or any Representatives have put in place in order to comply with this Agreement;
- 2.3.9 ensuring that the Conflicted Personnel and the Bid Team are line managed and report independently of each other; and
- 2.3.10 complying with any other action as the Authority, acting reasonably, may direct in connection with the ITT Process and/or this Agreement.

Notification of Conflicts of Interest**2.4 The Counterparty shall:**

- 2.4.1 notify the Authority immediately in writing of all perceived, potential and/or actual conflicts of interest that arise or have arisen;
- 2.4.2 submit in writing to the Authority full details of the nature of the perceived, potential and/or actual conflict of interest including full details of the risk assessments undertaken, the impact or potential impact of the perceived, potential and/or actual conflict, the measures and arrangements that have been established and/or are due to be established, to eliminate the perceived, potential and/or actual conflict, and the Counterparty's plans to prevent potential conflicts of interests from arising ("**Proposed Avoidance Measures**"); and
- 2.4.3 seek the Authority's approval to the Proposed Avoidance Measures which the Authority shall have the right to grant, grant conditionally or deny (if the Authority rejects the Proposed Avoidance Measures the Counterparty shall repeat the process set out in this Clause 2.4 until such time as the Authority grants approval or the Counterparty withdraws from the ITT Process).

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 2.5 The Counterparty will provide to the Authority, on demand, any and all information in relation to its adherence with its obligations set out under Clauses 2.2 and 2.3 as reasonably requested by the Authority.
- 2.6 The Authority reserves the right to require the Counterparty to demonstrate the measures put in place by the Counterparty under Clauses 2.2 and 2.3.
- 2.7 The Counterparty acknowledges that any provision of information or demonstration of measures, in accordance with Clauses 2.5 and 2.6, does not constitute acceptance by the Authority of the adequacy of such measures and does not discharge the Counterparty of its obligations or liability under this Agreement.

Exclusion from the ITT Process

- 2.8 Where, in the reasonable opinion of the Authority, there has been any breach by the Counterparty of Clauses 2.2, 2.3, or 2.4 or failure to obtain the Authority's approval of the Proposed Avoidance Measures the Authority shall be entitled to exclude the Counterparty, or any of its Affiliates and/or any Representatives, from the ITT Process, and the Authority may, in addition to the right to exclude, take such other steps as it deems necessary.
- 2.9 The actions of the Authority pursuant to Clause 2.8 shall not prejudice or affect any right of action or remedy under this Agreement or at law which shall have accrued or shall thereafter accrue to the Authority.

Bid Costs

- 2.10 In no event shall the Authority be liable for any bid costs incurred by:
- 2.10.1 the Counterparty or any of its Affiliates, any Representatives and/or any Subcontractors; or
- 2.10.2 any Third Party,
- as a result of any breach of this Agreement by the Counterparty, any of its Affiliates, any Subcontractors and/or Representatives, including where the Counterparty, any of its Affiliates, any Subcontractors or Representatives, or any Third Party is or are excluded from the ITT Process.

Specific Remedies

- 2.11 The Counterparty acknowledges and agrees that:
- 2.11.1 neither damages nor specific performance are adequate remedies in the event of a breach of the obligations in Clause 2; and
- 2.11.2 in the event of a breach of any of the obligations in Clause 2 which cannot be effectively remedied the Authority shall have the right to terminate

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

both this Agreement and the Counterparty's participation in the ITT Process in each case with immediate effect on written notice.

3 SOLE RESPONSIBILITY

- 3.1 It is the sole responsibility of the Counterparty to comply with the terms of this Agreement, including ensuring its Affiliates, any Subcontractors, and/or any Representatives comply with the terms of this Agreement. No approval by the Authority of any procedures, agreements or arrangements provided by the Counterparty, any of its Affiliates, any Subcontractors and/or their Representatives to the Authority shall discharge the Counterparty's obligations.

4 WAIVER AND INVALIDITY

- 4.1 No failure or delay by any Party in exercising any right, power or privilege under this Agreement or by law shall constitute a waiver of that or any other right, power or privilege, nor shall it restrict the further exercise of that or any other right, power or privilege. No single or partial exercise of such right, power or privilege shall prevent or restrict the further exercise of that or any other right, power or privilege.
- 4.2 If any provision of this Agreement is prohibited or unenforceable in any jurisdiction in relation to any Party, such prohibition or unenforceability will not invalidate the remaining provisions of this Agreement, or affect the validity or enforceability of the provisions of this Agreement in relation to any other Party or any other jurisdiction.

5 ASSIGNMENT AND NOVATION

- 5.1 The Counterparty shall not assign, novate or otherwise dispose of or create any trust in relation to any or all of its rights, obligations or liabilities under this Agreement without the prior written consent of the Authority.
- 5.2 The Authority may assign, novate or otherwise dispose of any or all of its rights, obligations and liabilities under this Agreement and/or any associated licences to:
- 5.2.1 any Central Government Body; or
 - 5.2.2 to a body other than a Central Government Body (including any private sector body) which performs any of the functions that previously had been performed by the Authority; and
 - 5.2.3 the Counterparty shall, at the Authority's request, enter into a novation agreement in such form as the Authority may reasonably specify in order to enable the Authority to exercise its rights pursuant to this Clause 5.
- 5.3 A change in the legal status of the Authority such that it ceases to be a Central Government Body shall not affect the validity of this Agreement and this Agreement shall be binding on any successor body to the Authority.

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

6 CONTRACTS (RIGHTS OF THIRD PARTIES) ACT 1999

- 6.1 A person who is not a Party to this Agreement has no right under the Contract (Rights of Third Parties) Act 1999 (as amended, updated or replaced from time to time) to enforce any term of this Agreement, but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.

7 TRANSPARENCY

- 7.1 The Parties acknowledge and agree that the Authority is under a legal duty pursuant to the Procurement Regulations to run transparent and fair procurement processes. Accordingly, the Authority may disclose the contents of this Agreement to Other Bidders (and/or potential Other Bidders) for the purposes of transparency and in order to evidence that a fair procurement process has been followed.

8 NOTICES

- 8.1 Any notices sent under this Agreement must be in writing.
- 8.2 The following table sets out the method by which notices may be served under this Agreement and the respective deemed time and proof of service:

Manner of Delivery	Deemed time of service	Proof of service
Email.	9.00am on the first Working Day after sending	Dispatched as a pdf attachment to an e-mail to the correct e-mail address without any error message.
Personal delivery.	On delivery, provided delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the next Working Day.	Properly addressed and delivered as evidenced by signature of a delivery receipt.
Prepaid, Royal Mail Signed For™ 1 st Class or other prepaid, next Working Day service providing proof of delivery.	At the time recorded by the delivery service, provided that delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery	Properly addressed prepaid and delivered as evidenced by signature of a delivery receipt.

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Manner of Delivery	Deemed time of service	Proof of service
	will occur at 9.00am on the same Working Day (if delivery before 9.00am) or on the next Working Day (if after 5.00pm).	

- 8.3 Notices shall be sent to the addresses set out below or at such other address as the relevant Party may give notice to the other Party for the purpose of service of notices under this Agreement:

	Counterparty	Authority
Contact		
Address		
Email		

- 8.4 This Clause 8 does not apply to the service of any proceedings or other documents in any legal action or other method of dispute resolution.

9 WAIVER AND CUMULATIVE REMEDIES

- 9.1 The rights and remedies under this Agreement may be waived only by notice, and in a manner that expressly states that a waiver is intended. A failure or delay by a Party in ascertaining or exercising a right or remedy provided under this Agreement or by law shall not constitute a waiver of that right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.
- 9.2 Unless otherwise provided in this Agreement, rights and remedies under this Agreement are cumulative and do not exclude any rights or remedies provided by law, in equity or otherwise.

10 TERM

- 10.1 Each Party's obligations under this Agreement shall continue in full force and effect for period of [] years from the Effective Date/[or for the period of the duration of the Procurement Process]

11 GOVERNING LAW AND JURISDICTION

- 11.1 This Agreement and any issues, disputes or claims (whether contractual or non-contractual) arising out of or in connection with it or its subject matter or formation

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

shall be governed by and construed in accordance with the laws of England and Wales.

11.2 The Parties agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (whether contractual or non-contractual) that arises out of or in connection with this Agreement or its subject matter or formation.

Signed by the Authority

Name:

Signature:

Position in Authority:

Signed by the Counterparty

Name:

Signature:

Position in Counterparty:

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 3: GUIDANCE FOR EXIT PLAN
Guidance for Supplier Contract Exit Plan11th October 2022, v0.3**Purpose**

This document provides a template (structure and headings) and guidance notes (level of detail and relationship to other sections) for the completion of the Exit Plan.

Assumption

The Exit Plan should be completed as a response to each transition plan provided by the Authority and/or Replacement Supplier(s). In the absence of a transition plan the Exit Plan should be completed based on the assumption that all Services will be transitioned as a single project, as quickly as possible, with the Supplier choosing the optimal service transition sequencing, highlighting service dependencies within the Exit Plan.

Example Table of Contents

- 1.0 Contents** [This template is the Table of Contents]
- 2.0 Glossary of Terms** [Includes both abbreviations and capitalised terms with their meaning]
- 3.0 Executive Summary** [maximum 5 pages]
 - 3.1 Objectives** [The detailed Exit Plan for all Services within the Contract]
 - 3.2 Milestone Exit Plan Summary** [Based on response to Section 8 below]
 - 3.3 Exit Charges Summary** [Based on response to Section 9 below]
- 4.0 Contract Life Obligations** [Links to the Registers content as per Schedule 10]
- 5.0 Exit Team Roles** [Includes roles/named individuals within the Supplier to support the Exit activities and governance model in Schedule 25 (Exit Management)]
 - 5.1 Supplier Management Structure**
 - 5.2 Supplier Roles & Responsibilities**
- 6.0 Scope** [The Supplier needs to define scope – this would include services provided as part of the original Agreement and changes made under change control (new, retired and revised scope items) through the contract life. Include any specific out-of-scope areas]
- 7.0 Exit Activities by Service**

[Describes activities to be completed by each party (Supplier, Authority and Replacement Suppliers) and the lead responsible party. To include:

 - any inter-dependencies between the Services.
 - any pre-requisites to exit one or more Services.

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- the approach to the closedown of Services.
- the approach to the secure destruction of Authority data to the Authority's Standards.
- the approach to equipment decommissioning of redundant equipment and materials, including environmental impact, to the Authority's requirements.

8.0 Exit Activities across Services

- the approach to transfer any available contracts to the Authority and/or the Replacement Supplier upon the expiry date together with any reasonable costs required to effect such transfer;
- proposals for the training of key members of the Replacement Supplier's staff in connection with the continuation of the provision of the Services following the expiry date;
- proposals for providing the Authority or a Replacement Supplier copies of all documentation relating to the use and operation of the Services and required for their continued use;
- proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Services;
- proposals for the identification and return of all Authority Assets in the possession of and/or control of the Supplier or any third party;
- how the Supplier will ensure that there is no disruption to or degradation of the Services during the Termination Assistance Period;
- any other information or assistance reasonably required by the Authority or a Replacement Supplier.
- programme management activities including the transfer of ongoing and planned inflight projects]

9.0 Exit Milestone Plan [Will include milestones, dependencies and timelines for the exit of all Services. To include Gantt chart providing an overview of the major milestones and activities by delivery/service area that would take place over the course of the contract exit.]

10.0 Exit Charges [Cost estimates for the exit of Services against the provided timeline. Includes stranded costs, estimated cost of Termination Services and any applicable reduction in charges as Services exit]

11.0 Authority Responsibilities [Any Authority responsibilities that the Supplier identifies to support the delivery of this Exit Plan. i.e. those identified by the Supplier over and above those already specified in this Contract]

12.0 Risk and Issues [Description of the current risks & issues related to contract exit using standard risk and issue registers. The risk register to include Event, Cause & Effect descriptions, Mitigation, Proximity, Likelihood Score, Impact Score, Owner, Overall Risk Score. For example, any risks or issues with

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

completing exit based on the Transition Plan provided by the Authority, if one is available]

13.0 Impact of Partial Exit [Description of how the Exit Plan would be impacted by a request by the Authority for the Supplier to exit a subset of the services provided under this Contract]

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 4
PRINCIPLES FOR DETERMINING CHARGES, COSTS AND EXPENSES IN
RELATION TO EXIT AND TERMINATION SERVICES

1. Save for where stated otherwise in this Schedule, the Supplier shall not be entitled to claim any additional charges, costs or expenses from the Authority in respect of:
 - a. its obligations under Paragraphs 2, 3, 4, 5, 7, 8 and 11 of this Schedule;
 - b. providing information, documentation and reports which are to be maintained or readily available as part of the contractual obligations during the Term which are, made available for exit related purposes under the terms of this Contract;
 - c. performing its obligations under this Contract relating to establishing and maintaining the Exit Plan;
 - d. providing information, documentation and reports for exit related purposes which can be produced without material incremental cost using information already held by the Supplier in the performance of this Contract;
 - e. exit related activities and support which can reasonably be provided using existing resources, including staff who are already providing the Services to perform such exit support and assistance without having a detrimental impact on the Services;
 - f. costs and expenses incurred by the Supplier as a result of its Defaults or delays in performing the exit and transfer Services save where such Defaults or delays are caused by the Authority and/or the Replacement Supplier(s) and/or any third parties engaged by the Authority;
 - g. providing reasonable escorted access to Supplier's Sites (subject to compliance with policies and procedures applicable at such premises and resources assigned to Services being available) for exit related purposes to the extent anticipated in the Exit Plan;
 - h. providing support or transfer to a Replacement Supplier for the Services or part thereof where the Supplier or any of its Affiliates will be the Replacement Supplier;
 - i. delivering one copy of the Authority's data to the Authority and/or the Replacement Supplier in a format which is based on the Government's Open Standards Principles (as described in Paragraph 4 (Open Data Standards & Standards Hub) of Schedule 4 (Standards));

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- j. ceasing all non-critical Software changes (except where agreed with the Authority in writing);
 - k. notifying the Sub-contractors of procedures to be followed during the Termination Assistance Period and providing management to ensure these procedures are followed;
 - l. providing Staffing Information in accordance with Schedule 28 (Staff Transfers);
 - m. compliance with regulatory obligations for staff transfer following the final agreement of staff transfer scope for role transfer to the Replacement Supplier;
 - n. providing the Authority with any problem logs pertaining to transferring services which have not previously been provided to the Authority;
 - o. reviewing all Software libraries used in connection with the transferring services and providing details of these to the Authority and/or the Replacement Supplier;
 - p. delivering to the Authority the existing systems support profiles, monitoring or systems logs (if required and where available), problem tracking/resolution documentation and status reports in respect of transferring Services; or
 - q. agreeing with the Authority a handover plan for all of the Supplier's responsibilities as set out in the Security Management Plan.
2. Termination Services provided by the Supplier during the Termination Assistance Period pursuant to this Schedule shall be chargeable as Time and Material Charges calculated in accordance with Paragraph 5 (Time and Material Charges) of Part A of Schedule 15 (Charges and Invoicing).
3. The Supplier shall use all reasonable endeavours to mitigate any costs and expenses incurred in relation to exit and/or the performance of the exit and transfer of the Services including, where possible, allocating existing resources in accordance with Paragraph 1(e) of this Annex 4.
4. The Authority shall be responsible for performing its obligations and ensuring that the Replacement Supplier(s) perform their obligations as and to the extent required for the planning and performance of the exit and transfer of the Services to the Replacement Supplier(s).

SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 5

DIAGRAM OF EXIT PROCESS DESCRIBED IN PARAGRAPH 11

NOTE: The diagram below has been included for illustration purposes only to summarise and illustrate the Partial Termination process for Services as set out in Paragraph 11 of this Schedule. In the event of any conflict or discrepancy between the diagram and Paragraph 11, Paragraph 11 shall take precedence.

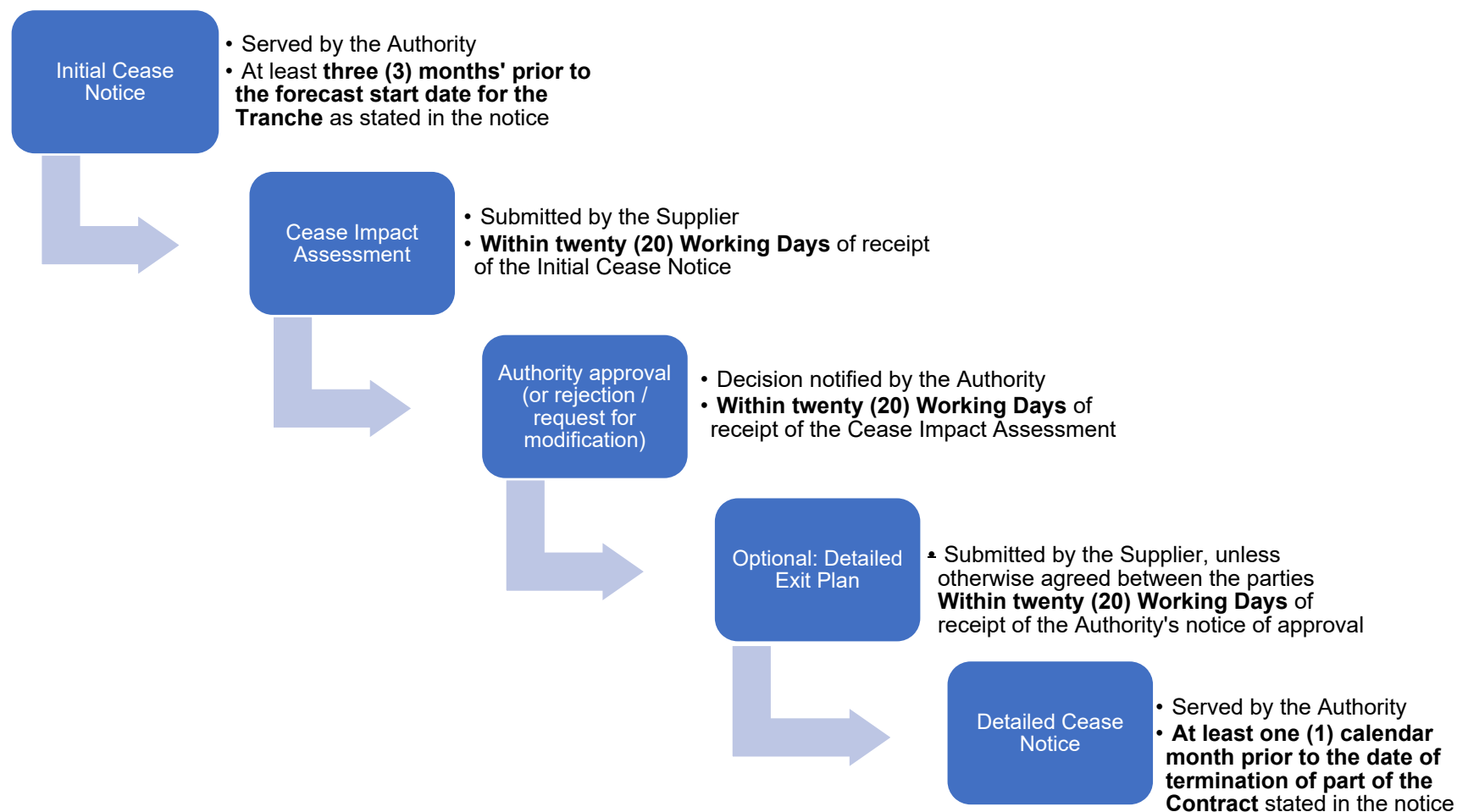
SCHEDULE 25 (EXIT MANAGEMENT)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]



**SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION
PLANNING)**

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 26

**SERVICE CONTINUITY PLAN AND CORPORATE
RESOLUTION PLANNING**

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Schedule 26 (Service Continuity Plan and Corporate Resolution Planning)

PART A: IT SERVICE CONTINUITY MANAGEMENT PLAN

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

“Department”	a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: (a) Government Department; or (b) Non-Ministerial Department.
“Disaster”	the occurrence of one or more events which, either separately or cumulatively, mean that the Services, or a material part of the Services will be unavailable for a period of time or which is reasonably anticipated will mean that the Services or a material part of the Services will be unavailable for a period or time or that there will be a significant degradation in performance of the Services or a material part of the Services;
“Disaster Recovery Plan”	a clearly defined and documented plan which recovers ICT capabilities when a disruption occurs;
“Disaster Recovery Services”	the services embodied in the processes and procedures for restoring the Services following the occurrence of a Disaster;
“Disaster Recovery System”	the system identified by the Supplier in the Supplier Solution which shall be used for the purpose of delivering the Disaster Recovery Services;
“Insolvency Continuity Plan”	has the meaning given in Paragraph 2.2(a)(iv).
“IT Service Continuity Management Plan”	means the plan prepared pursuant to Paragraph 2 of this Schedule which incorporates the ITSC

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Plan(s), Disaster Recovery Plan and the
Insolvency Continuity Plan;

- “ITSC Services”** has the meaning given in Paragraph 4.2(b);
- “Related Service Provider”** any person who provides services to the Authority in relation to this Contract from time to time, which persons include as at the Effective Date: VMED O2 UK Limited, British Telecom Plc, Vodafone Limited, Exponential-e Ltd , [REDACTED] and Ark Data Centres Limited ;
- “Review Report”** has the meaning given in Paragraphs 7.2(a) to 7.2(c);

2 IT SERVICE CONTINUITY MANAGEMENT PLAN

- 2.1 Within 40 Working Days from the Effective Date the Supplier shall prepare and deliver to the Authority for the Authority’s written approval a plan, which shall detail the processes and arrangements that the Supplier shall follow to:
- (a) ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Services (including where caused by an Insolvency Event of the Supplier, any Key Sub-contractor and/or any Supplier Group member); and
 - (b) the recovery of the Services in the event of a Disaster.
- 2.2 The IT Service Continuity Management Plan shall:
- (a) be divided into four parts:
 - (i) Part A which shall set out general principles and requirements applicable to the IT Service Continuity Management Plan;
 - (ii) Part B which shall relate to ITSC Plan(s);
 - (iii) Part C which shall relate to the Disaster Recovery Plan(s);
 - (iv) Part D which shall relate to an Insolvency Event of the Supplier, any Key Sub-contractors and/or any Supplier Group member (the **“Insolvency Continuity Plan”**); and
 - (b) unless otherwise required by the Authority in writing, be based upon and be consistent with the provisions of Paragraphs 3, 4, 5 and 6.

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 2.3 Following receipt of the draft IT Service Continuity Management Plan from the Supplier, the Authority shall:
- (a) review and comment on the draft IT Service Continuity Management Plan as soon as reasonably practicable; and
 - (b) notify the Supplier in writing that it approves or rejects the draft IT Service Continuity Management Plan no later than 20 Working Days after the date on which the draft Service Continuity Plan is first delivered to the Authority.
- 2.4 If the Authority rejects the draft IT Service Continuity Management Plan:
- (a) the Authority shall inform the Supplier in writing of its reasons for its rejection; and
 - (b) the Supplier shall then revise the draft IT Service Continuity Management Plan (taking reasonable account of the Authority's comments) and shall re-submit a revised draft IT Service Continuity Management Plan to the Authority for the Authority's approval within 20 Working Days of the date of the Authority's notice of rejection. The provisions of Paragraph 2.3 and this Paragraph 2.4 shall apply again to any resubmitted draft IT Service Continuity Management Plan, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.
- 3 IT SERVICE CONTINUITY MANAGEMENT PLAN: PART A – GENERAL PRINCIPLES AND REQUIREMENTS**
- 3.1 Part A of the IT Service Continuity Management Plan shall:
- (a) set out how the IT service continuity and disaster recovery elements of the plan link to each other;
 - (b) provide details of how the invocation of any element of the IT Service Continuity Management Plan may impact upon the operation of the Services and any services provided to the Authority by a Related Service Provider;
 - (c) contain an obligation upon the Supplier to liaise with the Authority and (at the Authority's request) any Related Service Provider with respect to issues concerning business continuity and disaster recovery where applicable;
 - (d) detail how the Service Continuity Plan links and interoperates with any overarching and/or connected disaster recovery, IT Service continuity plan of the Authority and any of its other Related Service Providers in each case as notified to the Supplier by the Authority from time to time;

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (e) contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multi-channels (including but without limitation a web-site (with FAQs), e-mail, phone and fax) for both portable and desk top configurations, where required by the Authority;
- (f) contain a risk analysis, including:
 - (i) failure or disruption scenarios and assessments and estimates of frequency of occurrence;
 - (ii) identification of any single points of failure within the Services and processes for managing the risks arising therefrom;
 - (iii) identification of risks arising from the interaction of the Services with the services provided by a Related Service Provider;
 - (iv) identification of risks arising from an Insolvency Event of the Supplier, any Key Sub-contractors and/or Supplier Group member; and
 - (v) a business impact analysis (detailing the impact on business processes and operations) of different anticipated failures or disruptions;
- (g) provide for documentation of processes, including business processes, and procedures;
- (h) set out key contact details (including roles and responsibilities) for the Supplier (and any Sub-contractors) and for the Authority;
- (i) identify the procedures for reverting to “normal service”;
- (j) set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to ensure that there is no more than the accepted amount of data loss and to preserve data integrity;
- (k) identify the responsibilities (if any) that the Authority has agreed it will assume in the event of the invocation of the IT Service Continuity Management Plan;
- (l) provide for the provision of technical advice and assistance to key contacts at the Authority as notified by the Authority from time to time to inform decisions in support of the Authority’s business continuity plans; and

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- (m) specify the standards, in addition to ISO/IEC 22301 and ISO/IEC 27031, that the IT Service Continuity Management is to be consistent with.
- 3.2 The IT Service Continuity Management Plan shall be designed so as to ensure that:
 - (a) the Services are provided in accordance with this Contract at all times during and after the invocation of the IT Service Continuity Management Plan;
 - (b) the adverse impact of any Disaster; service failure; an Insolvency Event of the Supplier, any Key Sub-contractor and/or any Supplier Group member; or disruption on the operations of the Authority, is minimal as far as reasonably possible;
 - (c) it complies with the relevant provisions of ISO/IEC 22301 and ISO/IEC 27031 and all other industry standards from time to time in force; and
 - (d) there is a process for the management of disaster recovery testing detailed in the IT Service Continuity Management Plan.
- 3.3 The IT Service Continuity Management Plan shall be upgradeable and sufficiently flexible to support any changes to the Services, to the business processes facilitated by and the business operations supported by the Services, and/or changes to the Supplier Group structure.
- 3.4 The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

4 IT SERVICE CONTINUITY MANAGEMENT PLAN: PART B – ITSC PLANS
PRINCIPLES AND CONTENTS

- 4.1 The ITSC Plan shall set out the arrangements that are to be invoked to ensure that the business processes and operations facilitated by the Services remain supported and to ensure continuity of the business operations supported by the Services including, unless the Authority expressly states otherwise in writing:
 - (a) the alternative processes (including business processes), options and responsibilities that may be adopted in the event of a failure in or disruption to the Services; and
 - (b) the steps to be taken by the Supplier upon resumption of the Services in order to address any prevailing effect of the failure or disruption including a root cause analysis of the failure or disruption.

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

4.2 The ITSC Plan shall:

- (a) address the various possible levels of failures of or disruptions to the Services;
- (b) set out the services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Services (such services and steps, the **"ITSC Services"**);
- (c) specify any applicable Performance Indicators with respect to the provision of the ITSC Services and details of any agreed relaxation to the Performance Indicators in respect of other Services during any period of invocation of the ITSC Plan; and
- (d) clearly set out the conditions and/or circumstances under which the ITSC Plan is invoked.

5 IT SERVICE CONTINUITY MANAGEMENT PLAN: PART C – DISASTER RECOVERY**PRINCIPLES AND CONTENTS**

- 5.1 The Disaster Recovery Plan shall be designed so as to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Authority supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.
- 5.2 The Disaster Recovery Plan shall be invoked only upon the occurrence of a Disaster.
- 5.3 The Disaster Recovery Plan shall include the following:
 - (a) the technical design and build specification of the Disaster Recovery System;
 - (b) details of the procedures and processes to be put in place by the Supplier in relation to the Disaster Recovery System and the provision of the Disaster Recovery Services and any testing of the same including but not limited to the following:
 - (i) data centre and disaster recovery site audits;
 - (ii) backup methodology and details of the Supplier's approach to data back-up and data verification;
 - (iii) identification of all potential disaster scenarios;
 - (iv) risk analysis;
 - (v) documentation of processes and procedures;
 - (vi) hardware configuration details;

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- (vii) network planning including details of all relevant data networks and communication links;
 - (viii) invocation rules;
 - (ix) Service recovery procedures; and
 - (x) steps to be taken upon resumption of the Services to address any prevailing effect of the failure or disruption of the Services;
- (c) any applicable Performance Indicators with respect to the provision of the Disaster Recovery Services and details of any agreed relaxation to the Performance Indicators in respect of other Services during any period of invocation of the Disaster Recovery Plan;
 - (d) details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;
 - (e) access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and
 - (f) testing and management arrangements.

6 SERVICE CONTINUITY PLAN: PART D – INSOLVENCY CONTINUITY PLAN**PRINCIPLES AND CONTENTS**

- 6.1 The Insolvency Continuity Plan shall be designed by the Supplier to permit continuity of the business operations of the Authority supported by the Services through continued provision of the Services following an Insolvency Event of the Supplier, any Key Sub-contractor and/or any Supplier Group member with, as far as reasonably possible, minimal adverse impact.
- 6.2 The Insolvency Continuity Plan shall include the following:
 - (a) communication strategies which are designed to minimise the potential disruption to the provision of the Services, including key contact details in respect of the supply chain and key contact details for operational and contract Supplier Personnel, Key Sub-contractor personnel and Supplier Group member personnel;
 - (b) identification, explanation, assessment and an impact analysis of risks in respect of dependencies between the Supplier, Key Sub-contractors and Supplier Group members where failure of those dependencies could reasonably have an adverse impact on the Services;
 - (c) plans to manage and mitigate identified risks;

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (d) details of the roles and responsibilities of the Supplier, Key Sub-contractors and/or Supplier Group members to minimise and mitigate the effects of an Insolvency Event of such persons on the Services;
- (e) details of the recovery team to be put in place by the Supplier (which may include representatives of the Supplier, Key Sub-contractors and Supplier Group members); and
- (f) sufficient detail to enable an appointed insolvency practitioner to invoke the plan in the event of an Insolvency Event of the Supplier.

7 REVIEW AND AMENDMENT OF THE IT SERVICE CONTINUITY MANAGEMENT PLAN

7.1 The Supplier shall review and update the IT Service Continuity Management Plan (and the risk analysis on which it is based):

- (a) on a regular basis and as a minimum once every 12 months;
- (b) within three calendar months of the IT Service Continuity Management Plan (or any part) having been invoked pursuant to Paragraph 9;
- (c) within 14 days of a Financial Distress Event;
- (d) within 30 days of a Corporate Change Event (unless the Relevant Authority (acting reasonably) agrees to a Corporate Change Event Grace Period, as set out in Paragraph 2.8(b)(i), in which case that Corporate Change Event Grace Period will apply);
- (e) where the Authority requests any additional reviews (over and above those provided for in Paragraphs 7.1(a) to 7.1(d)) by notifying the Supplier to such effect in writing, whereupon the Supplier shall conduct such reviews in accordance with the Authority's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Authority for the Authority's approval. The costs of both Parties of any such additional reviews shall be met by the Authority except that the Supplier shall not be entitled to charge the Authority for any costs that it may incur above any estimate without the Authority's prior written approval; and
- (f) following any change to the technical architecture of the service which impacts the resilience or recovery solutions.

7.2 Each review of the IT Service Continuity Management Plan pursuant to Paragraph 7.1 shall be a review of the procedures and methodologies set out in the IT Service Continuity Management Plan and shall assess their suitability having regard to any change to the Services or any underlying business processes and operations facilitated by or supported by the Services

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

which have taken place since the later of the original approval of the IT Service Continuity Management Plan or the last review of the IT Service Continuity Management Plan and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the IT Service Continuity Management Plan. The review shall be completed by the Supplier within the period required by the IT Service Continuity Management Plan or, if no such period is required, within such period as the Authority shall reasonably require. The Supplier shall, within 20 Working Days of the conclusion of each such review of the IT Service Continuity Management Plan, provide to the Authority a report (a "**Review Report**") setting out:

- (a) the findings of the review;
- (b) any changes in the risk profile associated with the Services; and
- (c) the Supplier's proposals (the "**Supplier's Proposals**") for addressing any changes in the risk profile and its proposals for amendments to the IT Service Continuity Management Plan following the review detailing the impact (if any and to the extent that the Supplier can reasonably be expected to be aware of the same) that the implementation of such proposals may have on any services or systems provided by a third party.

7.3 Following receipt of the Review Report and the Supplier's Proposals, the Authority shall:

- (a) review and comment on the Review Report and the Supplier's Proposals as soon as reasonably practicable; and
- (b) notify the Supplier in writing that it approves or rejects the Review Report and the Supplier's Proposals no later than 20 Working Days after the date on which they are first delivered to the Authority.

7.4 If the Authority rejects the Review Report and/or the Supplier's Proposals:

- (a) the Authority shall inform the Supplier in writing of its reasons for its rejection; and
- (b) the Supplier shall then revise the Review Report and/or the Supplier's Proposals as the case may be (taking reasonable account of the Authority's comments and carrying out any necessary actions in connection with the revision) and shall re-submit a revised Review Report and/or revised Supplier's Proposals to the Authority for the Authority's approval within 20 Working Days of the date of the Authority's notice of rejection. The provisions of Paragraph 7.3 and this Paragraph 7.4 shall apply again to any resubmitted Review Report and Supplier's Proposals, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 7.5 The Supplier shall as soon as is reasonably practicable after receiving the Authority's approval of the Supplier's Proposals (having regard to the significance of any risks highlighted in the Review Report) effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Services.

8 TESTING OF THE IT SERVICE CONTINUITY MANAGEMENT PLAN

- 8.1 The Supplier shall test the IT Service Continuity Management Plan on a regular basis (and in any event not less than once in every Contract Year). Subject to Paragraph 8.2, the Authority may require the Supplier to conduct additional tests of some or all aspects of the IT Service Continuity Management Plan at any time where the Authority considers it necessary, including where there has been any change to the Services or any underlying business processes, on the occurrence of any event which may increase the likelihood of the need to implement the IT Service Continuity Management Plan or following a live invocation of the IT Service Continuity Management Plan that has not been fully successful.
- 8.2 If the Authority requires an additional test of the IT Service Continuity Management Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Authority's requirements and the relevant provisions of the IT Service Continuity Management Plan. The Supplier's costs of the additional test shall be borne by the Authority unless the IT Service Continuity Management Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.
- 8.3 The Supplier shall undertake and manage testing of the IT Service Continuity Management Plan in full consultation with the Authority and shall liaise with the Authority in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Authority in this regard. Each test shall be carried out under the supervision of the Authority or its nominee.
- 8.4 The Supplier shall ensure that any use by it or any Sub-contractor of "live" data in such testing is first approved with the Authority. Copies of live test data used in any such testing shall be (if so required by the Authority) destroyed or returned to the Authority on completion of the test.
- 8.5 The Supplier shall, within 20 Working Days of the conclusion of each test, provide to the Authority a report setting out:
- (a) the outcome of the test;
 - (b) any failures in the IT Service Continuity Management Plan (including the Service Continuity Plan's procedures) revealed by the test; and
 - (c) the Supplier's proposals for remedying any such failures.

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 8.6 Following each test, the Supplier shall take all measures requested by the Authority, (including requests for the re-testing of the IT Service Continuity Management Plan) to remedy any failures in the IT Service Continuity Management Plan and such remedial activity and re-testing shall be completed by the Supplier, at no additional cost to the Authority, by the date reasonably required by the Authority and set out in such notice.
- 8.7 For the avoidance of doubt, the carrying out of a test of the IT Service Continuity Management Plan (including a test of the IT Service Continuity Management Plan's procedures) shall not relieve the Supplier of any of its obligations under this Contract.
- 8.8 The Supplier shall also perform a test of the IT Service Continuity Management Plan in the event of any major reconfiguration of the Services or as otherwise reasonably requested by the Authority.

9 INVOCATION OF THE IT SERVICE CONTINUITY MANAGEMENT PLAN

- 9.1 In the event of a loss of any critical part of the Service or a Disaster, the Supplier shall immediately invoke the business continuity and disaster recovery provisions in the IT Service Continuity Management Plan, including any linked elements in other parts of the IT Service Continuity Management Plan, and shall inform the Authority promptly of such invocation. In all other instances the Supplier shall invoke the ITSC and disaster recovery plan elements only with the prior consent of the Authority.
- 9.2 The Insolvency Continuity Plan element of the Service Continuity Plans, including any linked elements in other parts of the Service Continuity Plan, shall be invoked by the Supplier:
- (a) where an Insolvency Event of a Key Sub-contractor and/or Supplier Group member (other than the Supplier) could reasonably be expected to adversely affect delivery of the Services; and/or
 - (b) where there is an Insolvency Event of the Supplier and the insolvency arrangements enable the Supplier to invoke the plan;

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

PART B: CORPORATE RESOLUTION PLANNING**1 Service Status and Supplier Status**

- 1.1 This Contract is a Critical Service Contract.
- 1.2 The Supplier shall notify the Authority and the Cabinet Office Markets and Suppliers Team (Resolution.planning@cabinetoffice.gov.uk) in writing within 5 Working Days of the Effective Date and throughout the Term within 120 days after each Accounting Reference Date as to whether or not it is a Public Sector Dependent Supplier.

2 Provision of Corporate Resolution Planning Information (CRP Information)

- 2.1 Paragraphs 2 to 4 of this Part B shall apply if this Contract has been specified as a Critical Service Contract under Paragraph 1.1 of this Part B or the Supplier is or becomes a Public Sector Dependent Supplier.
- 2.2 Subject to Paragraphs 2.6, 2.10 and 2.11 of this Part B:
- (a) where this Contract is a Critical Service Contract, the Supplier shall provide the Relevant Authority or Relevant Authorities with CRP Information within 60 days of the Effective Date; and
 - (b) except where it has already been provided in accordance with Paragraph 2.2(a) of this Part B, where the Supplier is a Public Sector Dependent Supplier, it shall provide the Relevant Authority or Relevant Authorities with the CRP Information within 60 days of the date of the Relevant Authority's or Relevant Authorities' request.
- 2.3 The Supplier shall ensure that the CRP Information provided pursuant to Paragraphs 2.2, 2.8 and 2.9 of this Part B:
- (a) is full, comprehensive, accurate and up to date;
 - (b) is split into three parts:
 - (i) Exposure Information (Contracts List);
 - (ii) Corporate Resolvability Assessment (Structural Review);
 - (iii) Financial Information and Commentary
- and is structured and presented in accordance with the requirements and explanatory notes set out at the relevant Annex of the latest published versions of the Resolution Planning Guidance Notes published by the Cabinet Office Government Commercial Function and available at <https://www.gov.uk/government/publications/the-sourcing-and-consultancy-playbooks> and contains the level of detail required (adapted as necessary to the Supplier's circumstances);

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (c) incorporates any additional commentary, supporting documents and evidence which would reasonably be required by the Relevant Authority or Relevant Authorities to understand and consider the information for approval;
 - (d) provides a clear description and explanation of the Supplier Group members that have agreements for goods, services or works provision in respect of UK Public Sector Business and/or CNI and the nature of those agreements; and
 - (e) complies with the requirements set out at Annex 1 (*Exposure Information (Contracts List)*), Annex 2 (*Corporate Resolvability Assessment (Structural Review)*) and Annex 3 (*Financial Information And Commentary*) respectively.
- 2.4 Following receipt by the Relevant Authority or Relevant Authorities of the CRP Information pursuant to Paragraphs 2.2, 2.8 and 2.9 of this Part B, the Authority shall procure that the Relevant Authority or Relevant Authorities discuss in good faith the contents of the CRP Information with the Supplier and no later than 60 days after the date on which the CRP Information was delivered by the Supplier either provide an Assurance to the Supplier that Relevant Authority or Relevant Authorities approve the CRP Information or that Relevant Authority or Relevant Authorities reject the CRP Information.
- 2.5 If the Relevant Authority or Relevant Authorities reject the CRP Information:
- (a) the Authority shall (and shall procure that the Cabinet Office Markets and Suppliers Team shall) inform the Supplier in writing of its reasons for its rejection; and
 - (b) the Supplier shall revise the CRP Information, taking reasonable account of the Relevant Authority's or Relevant Authorities' comments, and shall re-submit the CRP Information to the Relevant Authority or Relevant Authorities for approval within 30 days of the date of the Relevant Authority's or Relevant Authorities' rejection. The provisions of Paragraph 2.3 to 2.5 of this Part B shall apply again to any resubmitted CRP Information provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.
- 2.6 Where the Supplier or a member of the Supplier Group has already provided CRP Information to a Department or the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely to the Cabinet Office Markets and Suppliers Team) and has received an Assurance of its CRP Information from that Department and the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely from the Cabinet Office Markets and Suppliers Team), then provided that the Assurance remains Valid on the date by which the CRP Information would otherwise be required, the Supplier shall not be required to provide the CRP Information under Paragraph 2.2 if it provides a copy of the Valid Assurance to the

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Relevant Authority or Relevant Authorities on or before the date on which the CRP Information would otherwise have been required.

- 2.7 An Assurance shall be deemed Valid for the purposes of Paragraph 2.6 of this Part B if:
- (a) the Assurance is within the validity period stated in the Assurance (or, if no validity period is stated, no more than 12 months has elapsed since it was issued and no more than 18 months has elapsed since the Accounting Reference Date on which the CRP Information was based); and
 - (b) no Corporate Change Events or Financial Distress Events (or events which would be deemed to be Corporate Change Events or Financial Distress Events if this Contract had then been in force) have occurred since the date of issue of the Assurance.
- 2.8 If this Contract is a Critical Service Contract, the Supplier shall provide an updated version of the CRP Information (or, in the case of Paragraph 2.8(c) of this Part B its initial CRP Information) to the Relevant Authority or Relevant Authorities:
- (a) within 14 days of the occurrence of a Financial Distress Event (along with any additional highly confidential information no longer exempted from disclosure under Paragraph 2.11 of this Part B) unless the Supplier is relieved of the consequences of the Financial Distress Event under Paragraph 7.1 of Schedule 18 (*Financial Distress*).
 - (b) within 30 days of a Corporate Change Event unless:
 - (i) the Supplier requests and the Relevant Authority (acting reasonably) agrees to a Corporate Change Event Grace Period, in the event of which the time period for the Supplier to comply with this Paragraph shall be extended as determined by the Relevant Authority (acting reasonably) but shall in any case be no longer than six months after the Corporate Change Event. During a Corporate Change Event Grace Period the Supplier shall regularly and fully engage with the Relevant Authority to enable it to understand the nature of the Corporate Change Event and the Relevant Authority shall reserve the right to terminate a Corporate Change Event Grace Period at any time if the Supplier fails to comply with this Paragraph; or
 - (ii) not required pursuant to Paragraph 2.10;
 - (c) within 30 days of the date that:

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (i) the credit rating(s) of each of the Supplier and its Parent Undertakings fail to meet any of the criteria specified in Paragraph 2.10; or
 - (ii) none of the credit rating agencies specified at Paragraph 2.10 hold a public credit rating for the Supplier or any of its Parent Undertakings; and
 - (d) in any event, within 6 months after each Accounting Reference Date or within 15 months of the date of the previous Assurance received from the Relevant Authority (whichever is the earlier), unless:
 - (i) updated CRP Information has been provided under any of Paragraphs 2.8(a) 2.8(b) or 2.8(c) since the most recent Accounting Reference Date (being no more than 12 months previously) within the timescales that would ordinarily be required for the provision of that information under this Paragraph 2.8(d); or
 - (ii) unless not required pursuant to Paragraph 2.10.
- 2.9 Where the Supplier is a Public Sector Dependent Supplier and this Contract is not a Critical Service Contract, then on the occurrence of any of the events specified in Paragraphs 2.8(a) to (d) of this Part B, the Supplier shall provide at the request of the Relevant Authority or Relevant Authorities and within the applicable timescales for each event as set out in Paragraph 2.8 (or such longer timescales as may be notified to the Supplier by the Authority), the CRP Information to the Relevant Authority or Relevant Authorities.
- 2.10 Where the Supplier or a Parent Undertaking of the Supplier has a credit rating of either:
- (a) [REDACTED] or better from Moody's; or
 - (b) [REDACTED] or better from Standard and Poor's; or
 - (c) [REDACTED] or better from Fitch; or
 - [REDACTED];
- the Supplier will not be required to provide any CRP Information unless or until either (i) a Financial Distress Event occurs (unless the Supplier is relieved of the consequences of the Financial Distress Event under Paragraph 7.1 of Schedule 18 (*Financial Distress*) or (ii) the Supplier and its Parent Undertakings cease to fulfil the criteria set out in this Paragraph 2.10, in which cases the Supplier shall provide the updated version of the CRP Information in accordance with Paragraph 2.8.
- 2.11 Subject to Paragraph 4, where the Supplier demonstrates to the reasonable satisfaction of the Relevant Authority or Relevant Authorities that a particular item of CRP Information is highly confidential, the Supplier may, having orally

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

disclosed and discussed that information with the Relevant Authority or Relevant Authorities, redact or omit that information from the CRP Information provided that if a Financial Distress Event occurs, this exemption shall no longer apply and the Supplier shall promptly provide the relevant information to the Relevant Authority or Relevant Authorities to the extent required under Paragraph 2.8.

3 Termination Rights

3.1 The Authority shall be entitled to terminate this Contract under Clause 31.1(b) (*Termination by the Authority*) if the Supplier is required to provide CRP Information under Paragraph 2 of this Part B and either:

- (a) the Supplier fails to provide the CRP Information within 4 months of the Effective Date if this is a Critical Service Contract or otherwise within 4 months of the Relevant Authority's or Relevant Authorities' request; or
- (b) the Supplier fails to obtain an Assurance from the Relevant Authority or Relevant Authorities within 4 months of the date that it was first required to provide the CRP Information under this Contract.

4 Confidentiality and usage of CRP Information

- 4.1 The Authority agrees to keep the CRP Information confidential and use it only to understand the implications of an Insolvency Event of the Supplier and/or Supplier Group members on its UK Public Sector Business and/or services in respect of CNI and to enable contingency planning to maintain service continuity for end users and protect CNI in such eventuality.
- 4.2 Where the Relevant Authority is the Cabinet Office Markets and Suppliers Team, at the Supplier's request, the Authority shall use reasonable endeavours to procure that the Cabinet Office enters into a confidentiality and usage agreement with the Supplier containing terms no less stringent than those placed on the Authority under Paragraph 4.1 of this Part B and Clause 19 (*Confidentiality*).
- 4.3 The Supplier shall use reasonable endeavours to obtain consent from any third party which has restricted the disclosure of the CRP Information to enable disclosure of that information to the Relevant Authority or Relevant Authorities pursuant to Paragraph 2 of this Part B subject, where necessary, to the Relevant Authority or Relevant Authorities entering into an appropriate confidentiality agreement in the form required by the third party.
- 4.4 Where the Supplier is unable to procure consent pursuant to Paragraph 4.3 of this Part B, the Supplier shall use all reasonable endeavours to disclose the CRP Information to the fullest extent possible by limiting the amount of information it withholds including by:

**SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION
PLANNING)**

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- (a) redacting only those parts of the information which are subject to such obligations of confidentiality
 - (b) providing the information in a form that does not breach its obligations of confidentiality including (where possible) by:
 - (i) summarising the information;
 - (ii) grouping the information;
 - (iii) anonymising the information; and
 - (iv) presenting the information in general terms
- 4.5 The Supplier shall provide the Relevant Authority or Relevant Authorities with contact details of any third party which has not provided consent to disclose CRP Information where that third party is also a public sector body and where the Supplier is legally permitted to do so.

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 1: EXPOSURE INFORMATION (CONTRACTS LIST)

- 1 The Supplier shall:
 - 1.1 provide details of all agreements held by members of the Supplier Group where those agreements are for goods, services or works provision and:
 - (a) are with any UK public sector bodies including: central Government departments and their arms-length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police fire and rescue, education bodies and the devolved administrations;
 - (b) are with any private sector entities where the end recipient of the service, goods or works provision is any of the bodies set out in Paragraph 1.1(a) of this Annex 1 and where the member of the Supplier Group is acting as a key sub-contractor under the agreement with the end recipient; or
 - (c) involve or could reasonably be considered to involve CNI;
 - 1.2 provide the Relevant Authority with a copy of the latest version of each underlying contract worth more than £5m per contract year and their related key sub-contracts, which shall be included as embedded documents within the CRP Information or via a directly accessible link.

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 2: CORPORATE RESOLVABILITY ASSESSMENT (STRUCTURAL REVIEW)

- 1 The Supplier shall:
 - 1.1 provide sufficient information to allow the Relevant Authority to understand the implications on the Supplier Group's UK Public Sector Business and CNI contracts listed pursuant to Annex 1 if the Supplier or another member of the Supplier Group is subject to an Insolvency Event.
 - 1.2 ensure that the information is presented so as to provide a simple, effective and easily understood overview of the Supplier Group; and
 - 1.3 provide full details of the importance of each member of the Supplier Group to the Supplier Group's UK Public Sector Business and CNI contracts listed pursuant to Annex 1 and the dependencies between each.

SCHEDULE 26 (SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 3: FINANCIAL INFORMATION AND COMMENTARY

- 1 The Supplier shall:
 - 1.1 provide sufficient financial information for the Supplier Group level, contracting operating entities level, and shared services entities' level to allow the Relevant Authority to understand the current financial interconnectedness of the Supplier Group and the current performance of the Supplier as a standalone entity; and
 - 1.2 ensure that the information is presented in a simple, effective and easily understood manner.
 - 1.3 For the avoidance of doubt the financial information to be provided pursuant to Paragraph 1 of this Annex 3 should be based on the most recent audited accounts for the relevant entities (or interim accounts where available) updated for any material changes since the Accounting Reference Date provided that such accounts are available in a reasonable timeframe to allow the Supplier to comply with its obligations under this Schedule 26 (Service Continuity Plan and Corporate Resolution Planning). If such accounts are not available in that timeframe, to the extent legally permissible financial information should be based on unpublished unaudited accounts or management accounts (disclosure of which to the Cabinet Office Markets and Suppliers Team remains protected by confidentiality).

SCHEDULE 27 (CONDUCT OF CLAIMS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 27

CONDUCT OF CLAIMS

SCHEDULE 27 (CONDUCT OF CLAIMS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 27 (Conduct of Claims)**1 INDEMNITIES**

- 1.1 This Schedule shall apply to the conduct, by a Party from whom an indemnity is sought under this Contract (the “**Indemnifier**”), of claims made by a third person against a party having (or claiming to have) the benefit of the indemnity (the “**Beneficiary**”).
- 1.2 If the Beneficiary receives any notice of any claim for which it appears that the Beneficiary is, or may become, entitled to indemnification under this Contract (a “**Claim**”), the Beneficiary shall give notice in writing to the Indemnifier as soon as reasonably practicable and in any event within 10 Working Days of receipt of the same.
- 1.3 Subject to Paragraph 2, on the giving of a notice by the Beneficiary, where it appears that the Beneficiary is or may be entitled to indemnification from the Indemnifier in respect of all (but not part only) of the liability arising out of the Claim, the Indemnifier shall (subject to providing the Beneficiary with a secured indemnity to its reasonable satisfaction against all costs and expenses that it may incur by reason of such action) be entitled to dispute the Claim in the name of the Beneficiary at the Indemnifier’s own expense and take conduct of any defence, dispute, compromise or appeal of the Claim and of any incidental negotiations relating to the Claim. If the Indemnifier does elect to conduct the Claim, the Beneficiary shall give the Indemnifier all reasonable cooperation, access and assistance for the purposes of such Claim and, subject to Paragraph 2.2, the Beneficiary shall not make any admission which could be prejudicial to the defence or settlement of the Claim without the prior written consent of the Indemnifier.
- 1.4 With respect to any Claim conducted by the Indemnifier pursuant to Paragraph 1.3:
- (a) the Indemnifier shall keep the Beneficiary fully informed and consult with it about material elements of the conduct of the Claim;
 - (b) the Indemnifier shall not bring the name of the Beneficiary into disrepute;
 - (c) the Indemnifier shall not pay or settle such Claim without the prior written consent of the Beneficiary, such consent not to be unreasonably withheld or delayed; and
 - (d) the Indemnifier shall conduct the Claim with all due diligence.
- 1.5 The Beneficiary shall be entitled to have conduct of the Claim and shall be free to pay or settle any Claim on such terms as it thinks fit and without prejudice to its rights and remedies under this Contract if:
- (a) the Indemnifier is not entitled to take conduct of the Claim in accordance with Paragraph 1.3;

SCHEDULE 27 (CONDUCT OF CLAIMS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (b) the Indemnifier fails to notify the Beneficiary in writing of its intention to take conduct of the relevant Claim within 10 Working Days of the notice from the Beneficiary or if the Indemnifier notifies the Beneficiary in writing that it does not intend to take conduct of the Claim; or
- (c) the Indemnifier fails to comply in any material respect with the provisions of Paragraph 1.4.

2 SENSITIVE CLAIMS

- 2.1 With respect to any Claim which the Beneficiary, acting reasonably, considers is likely to have an adverse impact on the general public's perception of the Beneficiary (a "**Sensitive Claim**"), the Indemnifier shall be entitled to take conduct of any defence, dispute, compromise or appeal of the Sensitive Claim only with the Beneficiary's prior written consent. If the Beneficiary withholds such consent and elects to conduct the defence, dispute, compromise or appeal of the Sensitive Claim itself, it shall conduct the Sensitive Claim with all due diligence and if it fails to do so, the Indemnifier shall only be liable to indemnify the Beneficiary in respect of that amount which would have been recoverable by the Beneficiary had it conducted the Sensitive Claim with all due diligence.
- 2.2 The Beneficiary shall be free at any time to give written notice to the Indemnifier that it is retaining or taking over (as the case may be) the conduct of any Claim, to which Paragraph 1.3 applies if, in the reasonable opinion of the Beneficiary, the Claim is, or has become, a Sensitive Claim.

3 RECOVERY OF SUMS

- 3.1 If the Indemnifier pays to the Beneficiary an amount in respect of an indemnity and the Beneficiary subsequently recovers (whether by payment, discount, credit, saving, relief or other benefit or otherwise) a sum which is directly referable to the fact, matter, event or circumstances giving rise to the Claim, the Beneficiary shall forthwith repay to the Indemnifier whichever is the lesser of:
 - (a) an amount equal to the sum recovered (or the value of the discount, credit, saving, relief, other benefit or amount otherwise obtained) less any out-of-pocket costs and expenses properly incurred by the Beneficiary in recovering or obtaining the same; and
 - (b) the amount paid to the Beneficiary by the Indemnifier in respect of the Claim under the relevant indemnity.

4 MITIGATION

- 4.1 Each of the Authority and the Supplier shall at all times take all reasonable steps to minimise and mitigate any loss for which the relevant Party is entitled to bring a claim against the other Party pursuant to the indemnities in this Schedule.

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 28

STAFF TRANSFER

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 28 (Staff Transfer)**1 DEFINITIONS**

1.1 In this Schedule, the following definitions shall apply:

“Admission Agreement”	the CSPA Admission Agreement (as defined in Annex D1: CSPA);
“Fair Deal Employees”	as defined in Part D;
“Former Supplier”	a supplier supplying services to the Authority or a Service Recipient before any Relevant Transfer Date that are the same as or substantially similar to the Services (or any part of the Services) and shall include any sub-contractor of such supplier (or any sub-contractor of any such sub-contractor);
“New Fair Deal”	the revised Fair Deal position set out in the HM Treasury guidance: <i>“Fair Deal for staff pensions: staff transfer from central government”</i> issued in October 2013 including: (a) any amendments to that document in force immediately prior to the Relevant Transfer Date; (b) any similar pension protection in accordance with the Annex D1 to Part D of this Schedule as notified to the Supplier by the Authority;
“Notified Sub-contractor”	a Sub-contractor identified in the Annex to this Schedule to whom Transferring Authority Employees or Transferring Former Supplier Employees will transfer on a Relevant Transfer Date;
“Old Fair Deal”	HM Treasury Guidance <i>“Staff Transfers from Central Government: A Fair Deal for Staff Pensions”</i> issued in June 1999 including the supplementary guidance <i>“Fair Deal for Staff pensions: Procurement of Bulk Transfer</i>

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Agreements and Related Issues” issued in June 2004;

“Replacement Sub-contractor”	a sub-contractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any sub-contractor of any such sub-contractor);
“Relevant Transfer”	a transfer of employment to which the Employment Regulations apply;
“Relevant Transfer Date”	in relation to a Relevant Transfer, the date upon which the Relevant Transfer takes place. For the purposes of Part D and its Annex, where the Supplier or a Sub-contractor was the Former Supplier and there is no Relevant Transfer of the Fair Deal Employees because they remain continuously employed by the Supplier (or Sub-contractor), references to the Relevant Transfer Date shall become references to the Operational Service Commencement Date;
“Service Transfer”	any transfer of the Services (or any part of the Services), for whatever reason, from the Supplier or any Sub-contractor to a Replacement Supplier or a Replacement Sub-contractor;
“Service Transfer Date”	the date of a Service Transfer or, if more than one, the date of the relevant Service Transfer as the context requires;
“Staffing Information”	in relation to all persons identified on the Supplier's Provisional Supplier Personnel List or Supplier's Final Supplier Personnel List, as the case may be, the information required in ANNEX E2: STAFFING INFORMATION in that format together with employee liability information specified in regulation 11(2) and 11(3) and if applicable 11(4) of the Employment Regulations and such other information as the Authority may reasonably require. The Authority may acting reasonably make changes to the format or information requested in ANNEX E2: STAFFING INFORMATION from time to time.
“Statutory Schemes”	means the CSPS, as defined in the Annex D1 to Part D of this Schedule;

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

“Supplier's Final Supplier Personnel List”	a list provided by the Supplier of all Supplier Personnel who will transfer under the Employment Regulations on the Service Transfer Date;
“Supplier's Provisional Supplier Personnel List”	a list prepared and updated by the Supplier of all Supplier Personnel who are at the date of the list wholly or mainly engaged in or assigned to the provision of the Services or any relevant part of the Services which it is envisaged as at the date of such list will no longer be provided by the Supplier following the Service Transfer Date;
“Transferring Former Supplier Employees”	in relation to a Former Supplier, those employees of the Former Supplier to whom the Employment Regulations will apply on the Relevant Transfer Date; and
“Transferring Supplier Employees”	those employees of the Supplier and/or of any Sub-contractors to whom the Employment Regulations will apply on the Service Transfer Date.

2 INTERPRETATION

- 2.1 Where a provision in this Schedule imposes an obligation on the Supplier to provide an indemnity, undertaking or warranty, the Supplier shall procure that each of its Sub-contractors shall comply with such obligation and provide such indemnity, undertaking or warranty to the Authority and any Service Recipient Former Supplier, Replacement Supplier or Replacement Sub-contractor, as the case may be.

3 APPLICABLE PARTS OF THIS SCHEDULE

- 3.1 Only the following parts of this Schedule shall apply to this Contract:
- (a) Part B (*Staff Transfer At Start Date – Transfer From Former Supplier*)
 - (b) Part C (*No Staff Transfer from Authority On Start Date*)
 - (c) Part D (*Pensions*)
 - (i) - Annex D1 (CSPS) may apply
 - (d) Part E (*Staff Transfer on Exit*)
 - (i) Annex E1 (*List Of Notified Sub-Contractors*)
 - (ii) Annex E2 (*Staffing Information*)

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

PART A: NOT USED

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

PART B: TRANSFERRING FORMER SUPPLIER EMPLOYEES AT COMMENCEMENT OF SERVICES**1 RELEVANT TRANSFERS**

1.1 The Authority and the Supplier agree that:

- (a) the commencement of the provision of the Services or of any relevant part of the Services may be a Relevant Transfer in relation to the Transferring Former Supplier Employees; and
- (b) as a result of the operation of the Employment Regulations, the contracts of employment between each Former Supplier and the Transferring Former Supplier Employees (except in relation to any terms disapplied through the operation of regulation 10 of the Employment Regulations) shall have effect on and from the Relevant Transfer Date as if originally made between the Supplier or Notified Sub-contractor (as the case may be) and each such Transferring Former Supplier Employee.

1.2 The Authority shall procure that each Former Supplier shall comply with all its obligations under the Employment Regulations and shall perform and discharge all its obligations in respect of all the Transferring Former Supplier Employees in respect of the period up to (but not including) the Relevant Transfer Date (including the payment of all remuneration, benefits, entitlements and outgoings, wages, accrued but untaken holiday pay, bonuses, commissions, payments of PAYE, national insurance contributions and pension contributions which in any case are attributable in whole or in part in respect of the period up to (but not including) the Relevant Transfer Date) and the Supplier shall make, and the Authority shall procure that each Former Supplier makes, any necessary apportionments in respect of any periodic payments.

2 FORMER SUPPLIER INDEMNITIES

2.1 Subject to Paragraph 2.2, the Authority shall procure that each Former Supplier shall indemnify the Supplier and any Notified Sub-contractor against any Employee Liabilities arising from or as a result of:

- (a) any act or omission by the Former Supplier in respect of any Transferring Former Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Former Supplier Employee arising before the Relevant Transfer Date;
- (b) the breach or non-observance by the Former Supplier arising before the Relevant Transfer Date of:
 - (i) any collective agreement applicable to the Transferring Former Supplier Employees; or

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (ii) any custom or practice in respect of any Transferring Former Supplier Employees which the Former Supplier is contractually bound to honour;
 - (c) any proceeding, claim or demand by HMRC or any other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:
 - (i) in relation to any Transferring Former Supplier Employee, to the extent that the proceeding, claim or demand by HMRC or such other statutory authority relates to financial obligations arising before the Relevant Transfer Date; and
 - (ii) in relation to any employee who is not a Transferring Former Supplier Employee and in respect of whom it is later alleged or determined that the Employment Regulations applied so as to transfer their employment from the Former Supplier to the Supplier or any Notified Sub-contractor, to the extent that the proceeding, claim or demand by HMRC or such other statutory authority relates to financial obligations in respect of the period up to (but not including) the Relevant Transfer Date;
 - (d) a failure of the Former Supplier to discharge or procure the discharge of all wages, salaries and all other benefits and all PAYE tax deductions and national insurance contributions relating to the Transferring Former Supplier Employees in respect of the period up to (but not including) the Relevant Transfer Date;
 - (e) any claim made by or in respect of any person employed or formerly employed by the Former Supplier other than a Transferring Former Supplier Employee for whom it is alleged the Supplier or any Notified Sub-contractor as appropriate may be liable by virtue of this Contract or the Employment Regulations; and
 - (f) any claim made by or in respect of a Transferring Former Supplier Employee or any appropriate representative (as defined in the Employment Regulations) of any Transferring Former Supplier Employee relating to any act or omission of the Former Supplier in relation to its obligations under regulation 13 of the Employment Regulations, except to the extent that the liability arises from the failure by the Supplier or any Sub-contractor to comply with regulation 13(4) of the Employment Regulations.
- 2.2 The indemnities in Paragraph 2.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to any act or omission of the Supplier or any Sub-contractor whether occurring or having its origin before, on or after the Relevant Transfer Date including, without limitation, any Employee Liabilities:

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (a) arising out of the resignation of any Transferring Former Supplier Employee before the Relevant Transfer Date on account of substantial detrimental changes to their working conditions proposed by the Supplier or any Sub-contractor to occur in the period from (and including) the Relevant Transfer Date; or
 - (b) arising from any failure by the Supplier or any Sub-contractor to comply with its obligations under the Employment Regulations.
- 2.3 If any person who is not identified as a Transferring Former Supplier Employee claims, or it is determined in relation to any such person that their contract of employment has been transferred from a Former Supplier to the Supplier or any Notified Sub-contractor pursuant to the Employment Regulations then:
 - (a) the Supplier shall, or shall procure that the Notified Sub-contractor shall, within 5 Working Days of becoming aware of that fact, give notice in writing to the Authority and, where required by the Authority, to the Former Supplier; and
 - (b) the Former Supplier may offer (or may procure that a third party may offer) employment to such person within 15 Working Days of the notification by the Supplier or the Notified Sub-contractor (as the case may be) or take such other reasonable steps as the Former Supplier considers appropriate to deal with the matter provided always that such steps are in compliance with applicable Law.
- 2.4 If an offer referred to in Paragraph 2.3(b) is accepted, or if the situation has otherwise been resolved by the Former Supplier or the Authority, the Supplier shall, or shall procure that the relevant Notified Sub-contractor shall, immediately release the person from their employment or alleged employment.
- 2.5 If by the end of the 15 Working Day period specified in Paragraph 2.3(b):
 - (a) no such offer of employment has been made;
 - (b) such offer has been made but not accepted; or
 - (c) the situation has not otherwise been resolved,the Supplier or the relevant Notified Sub-contractor may within 5 Working Days give notice to terminate the employment or alleged employment of such person.
- 2.6 Subject to the Supplier or any relevant Notified Sub-contractor (as the case may be) acting in accordance with the provisions of Paragraphs 2.3 to 2.5 and in accordance with all applicable proper employment procedures set out in Law, the Authority shall procure that the Former Supplier indemnifies the Supplier or any Notified Sub-contractor (as appropriate) against all Employee Liabilities arising out of the termination of employment pursuant to the provisions of Paragraph 2.5 provided that the Supplier takes, or (as the case

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

may be) procures that the relevant Notified Sub-contractor takes, all reasonable steps to minimise any such Employee Liabilities.

2.7 The indemnity in Paragraph 2.6:

(a) shall not apply to:

(i) any claim for:

(A) discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage, civil partnership, pregnancy, maternity or sexual orientation, religion or belief; or

(B) equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees,

in any case in relation to any alleged act or omission of the Supplier or any Sub-contractor; or

(ii) any claim that the termination of employment was unfair because the Supplier or the relevant Notified Sub-contractor neglected to follow a fair dismissal procedure; and

(b) shall apply only where the notification referred to in Paragraph 2.3(a) is made by the Supplier or the relevant Notified Sub-contractor (as the case may be) to the Authority and, if applicable, the Former Supplier, within 6 months of the relevant Relevant Transfer Date.

2.8 If any such person as is described in Paragraph 2.3 is neither re-employed by the Former Supplier nor dismissed by the Supplier or the relevant Notified Sub-contractor within the time scales set out in Paragraph 2.5, such person shall be treated as having transferred to the Supplier or that Notified Sub-contractor and the Supplier shall, or shall procure that the Notified Sub-contractor shall, (a) comply with such obligations as may be imposed upon it under the Law and (b) comply with the provisions of Part D (Pensions) and its Annex of this Staff Transfer Schedule.

3 SUPPLIER INDEMNITIES AND OBLIGATIONS

3.1 Subject to Paragraph 3.2, the Supplier shall indemnify the Authority or the Former Supplier against any Employee Liabilities arising from or as a result of:

(a) any act or omission by the Supplier or any Sub-contractor in respect of any Transferring Former Supplier Employee or any appropriate representative (as defined in the Employment Regulations) of any Transferring Former Supplier Employee whether occurring before, on or after the Relevant Transfer Date;

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (b) the breach or non-observance by the Supplier or any Sub-contractor on or after the Relevant Transfer Date of:
 - (i) any collective agreement applicable to the Transferring Former Supplier Employee; or
 - (ii) any custom or practice in respect of any Transferring Former Supplier Employees which the Supplier or any Sub-contractor is contractually bound to honour;
- (c) any claim by any trade union or other body or person representing any Transferring Former Supplier Employees arising from or connected with any failure by the Supplier or any Sub-contractor to comply with any legal obligation to such trade union, body or person arising on or after the Relevant Transfer Date;
- (d) any proposal by the Supplier or any Sub-contractor prior to the Relevant Transfer Date to make changes to the terms and conditions of employment or working conditions of any Transferring Former Supplier Employees to their material detriment on or after their transfer to the Supplier or a Sub-contractor (as the case may be) on the Relevant Transfer Date, or to change the terms and conditions of employment or working conditions of any person who would have been a Transferring Former Supplier Employee but for their resignation (or decision to treat their employment as terminated under regulation 4(9) of the Employment Regulations) before the Relevant Transfer Date as a result of or for a reason connected to such proposed changes;
- (e) any statement communicated by the Supplier or any Sub-contractor to, or action undertaken by the Supplier or any Sub-contractor to, or in respect of, any Transferring Former Supplier Employee before the Relevant Transfer Date regarding the Relevant Transfer which has not been agreed in advance with the Authority and the Former Supplier in writing;
- (f) any proceeding, claim or demand by HMRC or any other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:
 - (i) in relation to any Transferring Former Supplier Employee, to the extent that the proceeding, claim or demand by HMRC or such other statutory authority relates to financial obligations arising on or after the Relevant Transfer Date; and
 - (ii) in relation to any employee who is not a Transferring Former Supplier Employee, and in respect of whom it is later alleged or determined that the Employment Regulations applied so as to transfer their employment from the Former Supplier to the Supplier or a Sub-contractor, to the extent that the

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

proceeding, claim or demand by HMRC or such other statutory authority relates to financial obligations arising on or after the Relevant Transfer Date;

- (g) a failure of the Supplier or any Sub-contractor to discharge or procure the discharge of all wages, salaries and all other benefits and all PAYE tax deductions and national insurance contributions relating to the Transferring Former Supplier Employees in respect of the period from (and including) the Relevant Transfer Date;
 - (h) any claim made by or in respect of a Transferring Former Supplier Employee or any appropriate representative (as defined in the Employment Regulations) of any Transferring Former Supplier Employee relating to any act or omission of the Supplier or any Sub-contractor in relation to obligations under regulation 13 of the Employment Regulations, except to the extent that the liability arises from the Former Supplier's failure to comply with its obligations under regulation 13 of the Employment Regulations; and
 - (i) any failure by the Supplier or any Sub-Contractor to comply with its obligations under Paragraph 2.8 above
- 3.2 The indemnities in Paragraph 3.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Former Supplier whether occurring or having its origin before, on or after the Relevant Transfer Date including, without limitation, any Employee Liabilities arising from the Former Supplier's failure to comply with its obligations under the Employment Regulations.
- 3.3 The Supplier shall comply, and shall procure that each Sub-contractor shall comply, with all its obligations under the Employment Regulations (including without limitation its obligation to inform and consult in accordance with regulation 13 of the Employment Regulations) and shall perform and discharge, and shall procure that each Sub-contractor shall perform and discharge, all its obligations in respect of all the Transferring Former Supplier Employees, on and from the Relevant Transfer Date (including the payment of all remuneration, benefits, entitlements, outgoings, wages, accrued but untaken holiday pay, bonuses, commissions, payments of PAYE, national insurance contributions and pension contributions and any other sums due under the Admission Agreement which in any case are attributable in whole or in part to the period from (and including) the Relevant Transfer Date) and any necessary apportionments in respect of any periodic payments shall be made between the Supplier and the Former Supplier.

4 INFORMATION

- 4.1 The Supplier shall, and shall procure that each Sub-contractor shall, promptly provide to the Authority if the Authority so directs, to the Former Supplier, in writing such information as is necessary to enable the Former Supplier to carry out its duties under regulation 13 of the Employment Regulations. The Authority shall procure that the Former Supplier shall promptly provide to the

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Supplier and each Notified Sub-contractor in writing such information as is necessary to enable the Supplier and each Notified Sub-contractor to carry out their respective duties under regulation 13 of the Employment Regulations.

5 PRINCIPLES OF GOOD EMPLOYMENT PRACTICE

5.1 The Supplier shall, and shall procure that each Sub-contractor shall, comply with any requirement notified to it by the Authority relating to pensions in respect of any Transferring Former Supplier Employee as set down in:

- (a) the Cabinet Office Statement of Practice on Staff Transfers in the Public Sector of January 2000, revised December 2013;
- (b) Old Fair Deal; and
- (c) the New Fair Deal.

5.2 Any changes necessary to this Contract as a result of changes to or any replacement of in any statement of practice, paper or other guidance that replaces any of the documentation referred to in Paragraph 5.1 shall be agreed in accordance with the Change Control Procedure.

6 PROCUREMENT OBLIGATIONS

6.1 Notwithstanding any other provisions of this Part B, where in this Part B the Authority accepts an obligation to procure that a Former Supplier does or does not do something, such obligation shall be limited so that it extends only to the extent that the Authority's contract with the Former Supplier contains a contractual right in that regard which the Authority may enforce, or otherwise so that it requires only that the Authority must use reasonable endeavours to procure that the Former Supplier does or does not act accordingly.

7 PENSIONS

7.1 The Supplier shall, and shall procure that each Sub-contractor shall, comply as applicable with:

- (a) the requirements of Part 1 of the Pensions Act 2008, section 258 of the Pensions Act 2004 and the Transfer of Employment (Pension Protection) Regulations 2005 for all transferring staff; and
- (b) Part D (and its Annex) of this Staff Transfer Schedule.

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

PART C: NO TRANSFER OF AUTHORITY EMPLOYEES EXPECTED AT COMMENCEMENT OF SERVICES**1 PROCEDURE IN THE EVENT OF TRANSFER**

- 1.1 The Authority and the Supplier agree that the commencement of the provision of the Services or of any part of the Services is not expected to be a Relevant Transfer in relation to any employees of the Authority.
- 1.2 If any employee of the Authority claims, or it is determined in relation to any employee of the Authority, that their contract of employment has been transferred from the Authority to the Supplier or any Sub-contractor pursuant to the Employment Regulations then:
- (a) the Supplier shall, and shall procure that the relevant Sub-contractor shall, within 5 Working Days of becoming aware of that fact, give notice in writing to the Authority; and
 - (b) the Authority may offer (or may procure that a third party may offer) employment to such person within 15 Working Days of the notification by the Supplier or the Sub-contractor (as appropriate) or take such other reasonable steps as the Authority considers appropriate to deal with the matter provided always that such steps are in compliance with applicable Law.
- 1.3 If an offer referred to in Paragraph 1.2(b) is accepted (or if the situation has otherwise been resolved by the Authority, the Supplier shall, or shall procure that the Sub-contractor shall, immediately release the person from their employment or alleged employment.
- 1.4 If by the end of the 15 Working Day period specified in Paragraph 1.2(b):
- (a) no such offer of employment has been made;
 - (b) such offer has been made but not accepted; or
 - (c) the situation has not otherwise been resolved,
- the Supplier or the Sub-contractor (as the case may be) may within 5 Working Days give notice to terminate the employment or alleged employment of such person.

2 INDEMNITIES

- 2.1 Subject to the Supplier or the relevant Sub-contractor acting in accordance with the provisions of Paragraphs 1.2 to 1.4 and in accordance with all applicable employment procedures set out in applicable Law and subject also to Paragraph 2.4, the Authority shall indemnify the Supplier or the relevant Sub-contractor against all Employee Liabilities arising out of the termination of the employment of any employees of the Authority referred to in Paragraph 1.2 made pursuant to the provisions of Paragraph 1.4 provided that the Supplier

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

takes, or shall procure that the relevant Sub-contractor takes, all reasonable steps to minimise any such Employee Liabilities;

- 2.2 If any such person as is described in Paragraph 1.2 is neither re employed by the Authority or employed by any third party nor dismissed by the Supplier or any Sub-contractor within the 15 Working Day period referred to in Paragraph 1.4 such person shall be treated as having transferred to the Supplier or the Sub-contractor (as appropriate) and the Supplier shall, or shall procure that the Sub-contractor shall, comply with such obligations as may be imposed upon it under Law.
- 2.3 Where any person remains employed by the Supplier or any Sub-contractor pursuant to Paragraph 2.2, all Employee Liabilities in relation to such employee shall remain with the Supplier or the relevant Sub-contractor (as the case may be) and the Supplier shall indemnify the Authority, and shall procure that any relevant Sub-contractor shall indemnify the Authority, against any Employee Liabilities that the Authority may incur in respect of any such employees of the Supplier or employees of any Sub-contractor.
- 2.4 The indemnities in Paragraph 2.1:
- (a) shall not apply to:
 - (i) any claim for:
 - (A) discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage, civil partnership, pregnancy, maternity, sexual orientation, religion or belief; or
 - (B) equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees,

in any case in relation to any alleged act or omission of the Supplier or any Sub-contractor; or
 - (ii) any claim that the termination of employment was unfair because the Supplier or any relevant Sub-contractor neglected to follow a fair dismissal procedure; and
 - (b) shall apply only where the notification referred to in Paragraph 1.2(a) is made by the Supplier or any Sub-contractor to the Authority within 6 months of the relevant Relevant Transfer Date.

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

PART D: PENSIONS

1 DEFINITIONS

1.1 In this Part D and Part E, the following words have the following meanings and they shall supplement Schedule 1 (*Definitions*) and shall be deemed to include the definitions set out in the Annex to this Part D:

"Actuary" a Fellow of the Institute and Faculty of Actuaries;

"Admission Agreement" the CSPS Admission Agreement (as defined in Annex D1: CSPS);

"Broadly Comparable"

- (a) in respect of a pension scheme, a status satisfying the condition that there are no identifiable employees who will suffer material detriment overall in terms of future accrual of pension benefits as assessed in accordance with Annex A of New Fair Deal and demonstrated by the issue by the Government Actuary's Department of a broad comparability certificate; or
- (b) in respect of benefits provided for or in respect of a member under a pension scheme, benefits that are consistent with that pension scheme's certificate of broad comparability issued by the Government Actuary's Department,

and **"Broad Comparability"** shall be construed accordingly;

"CSPS" the schemes as defined in Annex D1 to this Part D;

"Fair Deal Eligible Employees" means the CSPS Eligible Employees (as defined in Annex D1 to this Part D), (and shall include any such employee who has been admitted to or remains eligible to join a Broadly Comparable pension scheme at the relevant time in accordance with Paragraph 10 or 11 of this Part D);

"Fair Deal Employees" any of:

- (a) Transferring Former Supplier Employees;
- (b) employees who are not Transferring Former Supplier Employees but to whom the Employment Regulations apply on the

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Relevant Transfer Date to transfer their employment to the Supplier or a Sub-Contractor, and whose employment is not terminated in accordance with the provisions of Paragraphs 2.5 of Parts B or Paragraph 1.4 of Part C; and

- (c) where the Supplier or a Sub-contractor was the Former Supplier, the employees of the Supplier (or Sub-contractor)

who at the Relevant Transfer Date are or become entitled to New Fair Deal protection in respect of any of the Statutory Schemes as notified by the Authority;

"New Fair Deal"

the revised Fair Deal position set out in the HM Treasury guidance: "*Fair Deal for Staff Pensions: Staff Transfer from Central Government*" issued in October 2013 including:

any amendments to that document in force immediately prior to the Relevant Transfer Date; and

any similar pension protection in accordance with Annex D1 inclusive as notified to the Supplier by the Authority.

2 PARTICIPATION

2.1 In respect of all or any Fair Deal Employees Annex D1: CSPS, shall apply, as appropriate.

2.2 The Supplier undertakes to do all such things and execute any documents (including any relevant Admission Agreement as may be required to enable the Supplier to participate in the appropriate Statutory Scheme in respect of the Fair Deal Employees and shall bear its own costs in such regard.

2.3 The Supplier undertakes:

- (a) to pay to the Statutory Schemes all such amounts as are due under the relevant Admission Agreement or otherwise and shall deduct and pay to the Statutory Schemes such employee contributions as are required; and
- (b) to be fully responsible for all other costs, contributions, payments and other amounts relating to its participation in the Statutory Schemes, including for the avoidance of doubt any exit payments and the costs of providing any bond, indemnity or guarantee required in relation to such participation.

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 2.4 Where the Supplier is the Former Supplier (or a Sub-contractor is a sub-contractor of the Former Supplier) and there is no Relevant Transfer of the Fair Deal Employees because they remain continuously employed by the Supplier (or Sub-contractor) at the Operational Service Commencement Date, this Part D and its Annex shall be modified accordingly so that the Supplier (or Sub-contractor) shall comply with its requirements from the Operational Service Commencement Date or, where it previously provided a Broadly Comparable pension scheme, from the date it is able to close accrual of its Broadly Comparable pension scheme (following appropriate consultation and contractual changes as appropriate) if later. The Supplier (or Sub-contractor) shall make arrangements for a bulk transfer from its Broadly Comparable pension scheme to the relevant Statutory Scheme in accordance with the requirements of the previous contract with the Authority.

3 PROVISION OF INFORMATION

- 3.1 The Supplier undertakes to the Authority:
- (a) to provide all information which the Authority may reasonably request concerning matters referred to in this Part D as expeditiously as possible;
 - (b) not to issue any announcements to any Fair Deal Employee prior to the Relevant Transfer Date concerning the matters stated in this Part D without the consent in writing of the Authority (such consent not to be unreasonably withheld or delayed); and
 - (c) retain such records as would be necessary to manage the pension aspects in relation to any current or former Fair Deal Eligible Employees arising on expiry or termination of this Contract.

4 INDEMNITIES

- 4.1 The Supplier shall indemnify and keep indemnified the Authority, any Replacement Supplier and any Replacement Sub-contractor on demand from and against all and any Losses whatsoever suffered or incurred by it or them which:
- (a) arise out of or in connection with any liability towards all and any Fair Deal Employees in respect of service on or after the Relevant Transfer Date which arises from any breach by the Supplier of this Part D, or the CSPS Admission Agreement; or
 - (b) relate to the payment of benefits under or participation in a pension scheme (as defined in section 150(1) Finance Act 2004) provided by the Supplier or a Sub-contractor on and after the Relevant Transfer Date until the date of termination or expiry of this Contract, including the Statutory Schemes or any Broadly Comparable pension scheme provided in accordance with Paragraphs 10 or 11 of this Part D; or
 - (c) relate to claims by Fair Deal Employees of the Supplier or of any Sub-contractor or by any trade unions, elected employee

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

representatives or staff associations in respect of all or any such Fair Deal Employees which Losses:

- (i) relate to any rights to benefits under a pension scheme (as defined in section 150(1) Finance Act 2004) in respect of periods of employment on and after the Relevant Transfer Date until the date of termination or expiry of this Contract; and
- (ii) arise out of the failure of the Supplier or any relevant Sub-contractor to comply with the provisions of this Part D before the date of termination or expiry of this Contract.

4.2 The indemnities in this Part D and its Annex:

- (a) shall survive termination of this Contract; and
- (b) shall not be affected by the caps on liability contained in Clause 23 (*Limitations on Liability*).

5 DISPUTES

5.1 The Dispute Resolution Procedure will not apply to any dispute (i) between the Authority and the Supplier or (ii) between their respective actuaries or (iii) between either or both of their respective actuaries about any of the actuarial matters referred to in this Part D and its Annex which shall in the absence of agreement between the Authority and the Supplier be referred to an independent Actuary:

- (a) who will act as an expert and not as an arbitrator;
- (b) whose decision will be final and binding on the Authority and the Supplier; and
- (c) whose expenses shall be borne equally by the Authority and the Supplier unless the independent Actuary shall otherwise direct.

5.2 The independent Actuary shall be agreed by the Parties or, failing such agreement the independent Actuary shall be appointed by the President for the time being of the Institute and Faculty of Actuaries on the application of the Parties.

6 THIRD PARTY RIGHTS

6.1 The Parties agree Clause 41 (*Third Party Rights*) does not apply and that the CRTPA applies to this Part D to the extent necessary to ensure that any Fair Deal Employee will have the right to enforce any obligation owed to or in respect of to them by the Supplier under this Part D, in their own right under section 1(1) of the CRTPA.

6.2 Further, the Supplier must ensure that the CRTPA will apply to any Sub-contract to the extent necessary to ensure that any Fair Deal Employee will

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

have the right to enforce any obligation owed to or in respect of them by the Sub-contractor in their own right under section 1(1) of the CRTPA.

7 BREACH

7.1 The Supplier agrees to notify the Authority should it breach any obligations it has under this Part D and agrees that the Authority shall be entitled to terminate this Contract for material Default in the event that the Supplier:

- (a) commits an irremediable breach of any provision of, or any obligation it has under this Part D; or
- (b) commits a breach of any provision of, or obligation it has under this Part D which, where capable of remedy, it fails to remedy within a reasonable time and in any event within 28 days of the date of a notice from the Authority giving particulars of the breach and requiring the Supplier to remedy it.

8 TRANSFER TO ANOTHER EMPLOYER/SUB-CONTRACTORS

8.1 Save on expiry or termination of this Contract, if the employment of any Fair Deal Eligible Employee transfers to another employer (by way of a transfer under the Employment Regulations or any other form of compulsory transfer of employment), the Supplier shall or shall procure that any relevant Sub-contractor shall:

- (a) notify the Authority as far as reasonably practicable in advance of the transfer to allow the Authority to make the necessary arrangements for participation in the relevant Statutory Schemes;
- (b) consult with those Fair Deal Employees about, and inform them of, the pension provisions relating to that transfer; and
- (c) procure that the employer to which those Fair Deal Eligible Employees are transferred (the "**New Employer**") complies with the provisions of this Part D and its Annex provided that references to the "Supplier" will become references to the New Employer, references to "Relevant Transfer Date" will become references to the date of the transfer to the New Employer and references to "Fair Deal Employees" will become references to the Fair Deal Eligible Employees so transferred to the New Employer.

9 PENSION ISSUES ON EXPIRY OR TERMINATION

9.1 The provisions of Part E: Staff Transfer on Exit (Mandatory) apply in relation to pension issues on expiry or termination of this Contract.

9.2 The Supplier shall (and shall procure that its Sub-contractors shall) prior to the termination of this Contract provide or procure all such co-operation and assistance (including co-operation and assistance from the Broadly Comparable pension scheme's Actuary) as the Replacement Supplier or CSPS or as the Authority may reasonably require, to enable the Replacement

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Supplier to participate in the appropriate Statutory Scheme in respect of any Fair Deal Eligible Employees that remains eligible for New Fair Deal protection following a Service Transfer.

10 BROADLY COMPARABLE PENSION SCHEME ON RELEVANT TRANSFER DATE

Not applicable

11 BROADLY COMPARABLE PENSION SCHEME IN OTHER CIRCUMSTANCES

11.1 If the terms of Paragraph 2.2 of Annex D1: CSPS, applies, the Supplier must (and must, where relevant, procure that each of its Sub-contractors will) ensure that, with effect from the cessation of participation in the Statutory Scheme, until the day before the Service Transfer Date, the relevant Fair Deal Eligible Employees will be eligible for membership of a pension scheme under which the benefits are Broadly Comparable to those provided under the relevant Statutory Scheme at the date of cessation of participation in the relevant Statutory Scheme, and then on such terms as may be decided by the Authority.

11.2 Such Broadly Comparable pension scheme must be:

- (a) established by the date of cessation of participation in the Statutory Scheme;
- (b) a registered pension scheme for the purposes of Part 4 of the Finance Act 2004;
- (c) capable of receiving a bulk transfer payment from the relevant Statutory Scheme (where instructed to do so by the Authority);
- (d) capable of paying a bulk transfer payment to the Replacement Supplier's Broadly Comparable pension scheme (or the relevant Statutory Scheme if applicable) (unless otherwise instructed by the Authority); and
- (e) maintained until such bulk transfer payments have been received or paid (as the case may be) (unless otherwise instructed by the Authority).or any

11.3 Where the Supplier Sub-contractor has provided a Broadly Comparable pension scheme pursuant to the provisions of this Paragraph 11, the Supplier shall (and, where a Sub-contractor has provided such a scheme, shall procure that any such Sub-contractor shall):

- (a) supply to the Authority details of its Broadly Comparable pension scheme and provide a full copy of the valid certificate of broad comparability (which remains valid as at the date of cessation of participation in the Statutory Scheme) covering all relevant Fair Deal Eligible Employees, as soon as it is able to do so before the

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

cessation of participation in the Statutory Scheme (where possible) and in any event no later than seven (7) days after receipt of the certificate;

- (b) be fully responsible for all costs, contributions, payments and other amounts relating to the setting up, certification of, ongoing participation in and withdrawal and exit from the Broadly Comparable pension scheme, including for the avoidance of doubt any debts arising under section 75 or 75A of the Pensions Act 1995;
- (c) where required to do so by the Authority, instruct any such Broadly Comparable pension scheme's Actuary to provide all such co-operation and assistance in agreeing a bulk transfer process as may be required by the Actuary to the relevant Statutory Scheme and to provide all such co-operation and assistance as may be required by any other Actuary appointed by the Authority (where applicable). The Supplier must ensure that day for day or pound for pound (as applicable) (or actuarially equivalent where there are benefit differences between the two schemes) credits in the Broadly Comparable pension scheme are provided in respect of any Fair Deal Employee who consents to such a transfer from the Statutory Scheme and the Supplier shall be fully responsible for any costs of providing those credits in excess of the bulk transfer payment received by the Broadly Comparable pension scheme; and
- (d) provide a replacement Broadly Comparable pension scheme in accordance with this Paragraph 11 with immediate effect for those Fair Deal Eligible Employees who are still employed by the Supplier or relevant Sub-contractor and are still eligible for New Fair Deal protection in the event that the Supplier's or Sub-contractor's Broadly Comparable pension scheme is closed to future accrual or terminated. The relevant Fair Deal Eligible Employees must be given the option to transfer their accrued benefits from the previous Broadly Comparable pension scheme to the new Broadly Comparable pension scheme on day for day or pound for pound terms (as applicable) (or actuarially equivalent where there are benefit differences between the two schemes).

- 11.4 Where the Supplier or any Sub-contractor has provided a Broadly Comparable pension scheme pursuant to the provisions of this Paragraph 11, the Supplier shall (and, where a Sub-contractor has provided such a scheme, shall procure that any such Sub-contractor shall) prior to the termination of this Contract allow and make all necessary arrangements to effect, in respect of any Fair Deal Eligible Employee that remains eligible for New Fair Deal protection, following a Service Transfer, the bulk transfer of past service from any such Broadly Comparable pension scheme into the Replacement Supplier's Broadly Comparable pension scheme (or relevant Statutory Scheme if applicable). The bulk transfer terms provided shall be sufficient to secure day for day or pound for pound credits (as applicable) (or actuarially equivalent where there are benefit differences between the two schemes) in the Replacement Supplier's

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Broadly Comparable pension scheme (or relevant Statutory Scheme if applicable). For the avoidance of doubt, should the amount offered by the Broadly Comparable pension scheme be less than the amount required by the Replacement Supplier's Broadly Comparable pension scheme (or the relevant Statutory Scheme if applicable) to fund the required credits ("**the Shortfall**"), the Supplier or any such Sub-contractor (as agreed between them) must pay the Replacement Supplier's Broadly Comparable pension scheme (or relevant Statutory Scheme if applicable) the Shortfall as required, provided that in the absence of any agreement between the Supplier and any such Sub-contractor, the Shortfall shall be paid in full by the Supplier. The Supplier shall indemnify the Authority and the Replacement Supplier's Broadly Comparable pension scheme (or the relevant Statutory Scheme if applicable) (as the Authority directs) for any failure to pay the Shortfall under this Paragraph.

12 RIGHT OF SET-OFF

- 12.1 The Authority shall at any time have a right to set off against any payments due to the Supplier under this Contract an amount equal to any unpaid employer's contributions or employee's contributions or any other financial obligations under the CSPS or any CSPS Admission Agreement in respect of the CSPS Eligible Employees whether due from the Supplier or any relevant Sub-contractor or from any third party under any indemnity, bond or guarantee, and shall pay such set off amount to the relevant Statutory Scheme.
- 12.2 The Authority shall also have a right to set off against any payments due to the Supplier under this Contract all reasonable costs and expenses incurred by the Authority as result of the application of Paragraphs 12.1 above.

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX D1: CSPA**1 DEFINITIONS**

- 1.1 In this Annex D1: CSPA to Part D: Pensions, the following words have the following meanings:

"CSPA Admission Agreement"	an admission agreement in the form available on the Civil Service Pensions website immediately prior to the Relevant Transfer Date to be entered into for the CSPA in respect of the Services;
"CSPA Eligible Employee"	any CSPA Fair Deal Employee who at the relevant time is an active member of, or eligible to participate in the CSPA under a CSPA Admission Agreement;
"CSPA Fair Deal Employee"	a Fair Deal Employee who at the Relevant Transfer Date is or becomes entitled to protection in respect of the CSPA in accordance with the provisions of New Fair Deal;
"CSPA"	the "Alpha" introduced under The Public Service (Civil Servants and Others) Pensions Regulations 2014, available to Civil Servants and employees of bodies under Schedule 1 of the Superannuation Act 1972 (and eligible employees of other bodies admitted to participate under a determination under section 25 of the Public Service Pensions Act 2013), as governed by rules adopted by Parliament; the Partnership Pension Account and its (i) Ill health Benefits Arrangements and (ii) Death Benefits Arrangements; the Civil Service Additional Voluntary Contribution Scheme.

2 FUTURE SERVICE BENEFITS

- 2.1 In accordance with New Fair Deal, the Supplier and any of its Sub-contractors to which the employment of any CSPA Fair Deal Employee compulsorily transfers as a result of either the award of this Contract or a Relevant Transfer, if not an employer which participates automatically in the CSPA, shall each secure a CSPA Admission Agreement to ensure that CSPA Fair Deal Employees or CSPA Eligible Employees as appropriate shall be either admitted into, or offered continued membership of, the relevant section of the CSPA to which they currently contribute, or were eligible to join immediately prior to the Relevant Transfer Date or became eligible to join on the Relevant Transfer Date. The Supplier will and will procure that any such Sub-contractors will ensure that the CSPA Fair Deal Employees continue to accrue benefits in the CSPA in accordance with the provisions governing the relevant

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

section of the CSPA for service from (and including) the Relevant Transfer Date.

- 2.2 If the Supplier or any of its Sub-contractors enters into a CSPA Admission Agreement in accordance with Paragraph 2.1 but the CSPA Admission Agreement is terminated during the term of this Contract for any reason at a time when the Supplier or Sub-contractor still employs any CSPA Eligible Employees, the Supplier shall and shall procure that any relevant Sub-contractors shall, at no extra cost to the Authority, offer the remaining CSPA Eligible Employees membership of a pension scheme which is Broadly Comparable to the CSPA on the date those CSPA Eligible Employees ceased to participate in the CSPA, in accordance with the provisions of Paragraph 11 of Part D.

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

PART E: EMPLOYMENT EXIT PROVISIONS**1 PRE-SERVICE TRANSFER OBLIGATIONS**

1.1 The Supplier agrees that within 20 Working Days of the earliest of:

- (a) receipt of a notification from the Authority of a Service Transfer or intended Service Transfer;
- (b) receipt of the giving of notice of early termination or any Partial Termination of this Contract; and
- (c) the date which is 12 months before the end of the Term; or
- (d) receipt of a written request by the Authority at any time (provided that the Authority shall only be entitled to make one such request in any 6 month period),

it shall provide in a suitably anonymised format so as to comply with the DPA 2018, the Supplier's Provisional Supplier Personnel List, together with the Staffing Information and it shall provide an updated Supplier's Provisional Supplier Personnel List at such intervals as are reasonably requested by the Authority.

1.2 At least 20 Working Days prior to the Service Transfer Date, the Supplier shall provide to the Authority or at the direction of the Authority to any Replacement Supplier or Replacement Sub-contractor:

- (a) the Supplier's Final Supplier Personnel List, which shall identify which of the Supplier Personnel are Transferring Supplier Employees; and
- (b) the Staffing Information in relation to the Supplier's Final Supplier Personnel List (insofar as such information has not previously been provided).

1.3 The Authority shall be permitted to use and disclose information provided by the Supplier under Paragraphs 1.1 and 1.2 for the purpose of informing any prospective Replacement Supplier or Replacement Sub-contractor.

1.4 The Supplier warrants, for the benefit of the Authority, any Replacement Supplier, and any Replacement Sub-contractor that all information provided pursuant to Paragraphs 1.1 and 1.2 shall be complete, true and accurate in all material respects at the time of providing the information.

1.5 From the date of the earliest event referred to in Paragraph 1.1(a), 1.1(b) and 1.1(c), the Supplier agrees, that it shall not, and shall procure that each Sub-contractor shall not, assign any person to the provision of the Services who is not listed on the Supplier's Provisional Supplier Personnel List and shall not without the prior approval of the Authority (not to be unreasonably withheld or delayed):

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (a) replace or re-deploy any Supplier Personnel listed on the Supplier's Provisional Supplier Personnel List other than where any replacement is of equivalent grade, skills, experience and expertise and is employed on the same terms and conditions of employment as the person they replace;
- (b) make, promise, propose, permit or implement any material changes to the terms and conditions of employment of the Supplier Personnel (including pensions and any payments connected with the termination of employment);
- (c) increase the proportion of working time spent on the Services (or the relevant part of the Services) by any of the Supplier Personnel save for fulfilling assignments and projects previously scheduled and agreed;
- (d) introduce any new contractual or customary practice concerning the making of any lump sum payment on the termination of the employment or engagement of any person listed on the Supplier's Provisional Supplier Personnel List;
- (e) increase or reduce the total number of persons so engaged or deploy any other person to perform the Services (or the relevant part of the Services); or
- (f) terminate or give notice to terminate the employment or engagement of any person on the Supplier's Provisional Supplier Personnel List, save by due disciplinary process,

and shall promptly notify, and procure that each Sub-contractor shall promptly notify, the Authority and, at the direction of the Authority, any Replacement Supplier and any Replacement Sub-contractor, of any notice given or received by the Supplier or any Sub-contractor to terminate the employment or engagement of any person listed on the Supplier's Provisional Supplier Personnel List, regardless of when such notice takes effect.

1.6 During the Term, the Supplier shall provide, and shall procure that each Sub-contractor shall provide, within 20 Working Days to the Authority any information the Authority may reasonably require relating to the manner in which the Services are organised, which shall include:

- (a) the numbers of Supplier Personnel engaged in providing the Services;
- (b) the percentage of time spent by each Supplier Personnel engaged in providing the Services;
- (c) the extent to which each employee qualifies for membership of any of the Statutory Schemes or any Broadly Comparable scheme set up pursuant to the provisions of the Annex D1 to Part D (*Pensions*) of this Schedule 28 (Staff Transfer) (as appropriate);

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (d) a description of the nature of the work undertaken by each Supplier Personnel by location.
- 1.7 The Supplier shall provide, and shall procure that each Sub-contractor shall provide, all reasonable cooperation and assistance to the Authority, any Replacement Supplier and any Replacement Sub-contractor to ensure the smooth transfer of the Transferring Supplier Employees on the Service Transfer Date including providing sufficient information in advance of the Service Transfer Date to ensure that all necessary payroll arrangements can be made to enable the Transferring Supplier Employees to be paid as appropriate. Without prejudice to the generality of the foregoing, within 5 Working Days following the Service Transfer Date, the Supplier shall provide, and shall procure that each Sub-contractor shall provide, to the Authority and at the direction of the Authority, to any Replacement Supplier and any Replacement Sub-contractor, in respect of each person on the Supplier's Final Supplier Personnel List who is a Transferring Supplier Employee:
- (a) the most recent month's copy pay slip data;
 - (b) details of cumulative pay for tax and pension purposes;
 - (c) details of cumulative tax paid;
 - (d) confirmation that details of the tax codes have been provided and confirmed or amended;
 - (e) confirmation that details of any voluntary deductions from pay have been provided and confirmed or amended;
 - (f) a copy of any personnel file and/or any other records regarding the service of the Transferring Supplier Employee;
 - (g) a complete copy of the information required to meet the minimum recording keeping requirements under the Working Time Regulations 1998 and the National Minimum Wage Regulations 1998; and
 - (h) confirmation that bank/building society account details for payroll purposes have been provided and confirmed or amended.
- 1.8 From the date of the earliest event referred to in Paragraph 1.1(a), 1.1(b) and 1.1(c) the Supplier agrees that following a request from the Authority it shall and shall procure that each Sub-contractor shall use reasonable endeavours to comply with any request to align and assign Supplier Personnel to any future delivery model proposed by the Authority for Replacement Services within 30 Working Days or such longer timescale as may be agreed.
- 1.9 Any changes necessary to this Contract as a result of alignment referred to in Paragraph 1.8 shall be agreed in accordance with the Change Control Procedure.

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

2 EMPLOYMENT REGULATIONS EXIT PROVISIONS

- 2.1 The Authority and the Supplier acknowledge that subsequent to the commencement of the provision of the Services, the identity of the provider of the Services (or any part of the Services) may change (whether as a result of termination or Partial Termination of this Contract or otherwise) resulting in the Services (or any part of the Services) being undertaken by a Replacement Supplier or a Replacement Sub-contractor. Such change in the identity of the supplier of such services may constitute a Relevant Transfer to which the Employment Regulations will apply. The Authority and the Supplier agree that, as a result of the operation of the Employment Regulations, where a Relevant Transfer occurs, the contracts of employment between the Supplier and the Transferring Supplier Employees (except in relation to any contract terms disapplied through the operation of regulation 10 of the Employment Regulations) will have effect on and from the Service Transfer Date as if originally made between the Replacement Supplier or the relevant Replacement Sub-contractor (as the case may be) and each such Transferring Supplier Employee.
- 2.2 The Supplier shall, and shall procure that each Sub-contractor shall, comply with all its obligations under the Employment Regulations and in particular obligations in respect of the Transferring Supplier Employees arising under the Employment Regulations in respect of the period up to (but excluding) the Service Transfer Date and shall perform and discharge, and procure that each Sub-contractor shall perform and discharge, all its obligations in respect of any person identified in Supplier's Final Supplier Personnel List arising in respect of the period up to (but excluding) the Service Transfer Date (including the payment of all remuneration, benefits, entitlements and outgoings, wages, pay for accrued but untaken holiday, bonuses, commissions, payments of PAYE, national insurance contributions, pension contributions and all such sums due as a result of any Fair Deal Employees' participation in the Schemes which in any case are attributable in whole or in part to the period ending on (but excluding) the Service Transfer Date) and any necessary apportionments in respect of any periodic payments shall be made between: (i) the Supplier or the relevant Sub-contractor (as appropriate) and (ii) the Replacement Supplier or the relevant Replacement Sub-contractor (as appropriate).
- 2.3 Subject to Paragraph 2.4, the Supplier shall indemnify the Authority and the Replacement Supplier and any Replacement Sub-contractor against all and any Employee Liabilities arising from or as a result of:
- (a) any act or omission of the Supplier or any Sub-contractor in respect of any Transferring Supplier Employee or any appropriate representative (as defined in the Employment Regulations) of any Transferring Supplier Employee whether occurring before, on or after the Service Transfer Date;
 - (b) the breach or non-observance by the Supplier or any Sub-contractor occurring before but excluding the Service Transfer Date of:

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (i) any collective agreement applicable to the Transferring Supplier Employees; or
 - (ii) any custom or practice in respect of any Transferring Supplier Employees which the Supplier or any Sub-contractor is contractually bound to honour;
- (c) any claim by any trade union or other body or person representing any Transferring Supplier Employees arising from or connected with any failure by the Supplier or any Sub-contractor to comply with any legal obligation to such trade union, body or person arising before but excluding the Service Transfer Date;
- (d) any proceeding, claim or demand by HMRC or any other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:
 - (i) in relation to any Transferring Supplier Employee, to the extent that the proceeding, claim or demand by HMRC or such other statutory authority relates to financial obligations arising before but excluding the Service Transfer Date; and
 - (ii) in relation to any employee who is not identified in the Supplier's Final Supplier Personnel List, and in respect of whom it is later alleged or determined that the Employment Regulations applied so as to transfer their employment from the Supplier to the Authority or any Replacement Supplier or Replacement Sub-contractor, to the extent that the proceeding, claim or demand by HMRC or such other statutory authority relates to financial obligations arising before but excluding the Service Transfer Date;
- (e) a failure of the Supplier or any Sub-contractor to discharge or procure the discharge of all wages, salaries and other benefits and all PAYE tax deductions and national insurance contributions relating to the Transferring Supplier Employees in respect of the period up to (but excluding) the Service Transfer Date);
- (f) any claim made by or in respect of any person employed or formerly employed by the Supplier or any Sub-contractor other than a Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List for whom it is alleged the Authority or any the Replacement Supplier or Replacement Sub-contractor may be liable by virtue of this Contract or the Employment Regulations; and
- (g) any claim made by or in respect of a Transferring Supplier Employee or any appropriate representative (as defined in the Employment Regulations) of any Transferring Supplier Employee relating to any act or omission of the Supplier or any Sub-contractor in relation to its obligations under regulation 13 of the Employment

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Regulations, except to the extent that the liability arises from the failure by the Authority or any Replacement Supplier or Replacement Sub-contractor to comply with regulation 13(4) of the Employment Regulations.

- 2.4 The indemnities in Paragraph 2.3 shall not apply to the extent that the Employee Liabilities arise or are attributable to any act or omission of any Replacement Supplier or Replacement Sub-contractor, whether occurring or having its origin before, on or after the Service Transfer Date, including any Employee Liabilities:
- (a) arising out of the resignation of any Transferring Supplier Employee before the Service Transfer Date on account of substantial detrimental changes to their working conditions proposed by any Replacement Supplier or Replacement Sub-contractor to occur in the period on or after the Service Transfer Date); or
 - (b) arising from any failure by any Replacement Supplier or Replacement Sub-contractor to comply with its obligations under the Employment Regulations.
- 2.5 If any person who is not identified in the Supplier's Final Supplier Personnel List claims, or it is determined in relation to any such person, that their contract of employment has been transferred from the Supplier or any Sub-contractor to any Replacement Supplier or Replacement Sub-contractor pursuant to the Employment Regulations:
- (a) the Authority shall procure that the relevant Replacement Supplier or Replacement Sub-contractor shall, within 5 Working Days of becoming aware of that fact, give notice of it in writing to the Supplier; and
 - (b) the Supplier may offer (or may procure that a Sub-contractor may offer) employment to such person within 15 Working Days of the notification by the Replacement Supplier or Replacement Sub-contractor (as the case may be) or take such other reasonable steps as it considers appropriate to deal with the matter provided always that such steps are in compliance with Law
- 2.6 If such offer is accepted, or if the situation has otherwise been resolved by the Supplier or any Sub-contractor, the Authority shall procure that the relevant Replacement Supplier or Replacement Sub-contractor shall immediately release or procure the release of the person from their employment or alleged employment.
- 2.7 If after the 15 Working Day period specified in Paragraph 2.5(b) has elapsed:
- (a) no such offer of employment has been made;
 - (b) such offer has been made but not accepted; or

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

(c) the situation has not otherwise been resolved

the Authority shall advise the relevant Replacement Supplier or Replacement Sub-contractor that it may within 5 Working Days give notice to terminate the employment or alleged employment of such person.

2.8 Subject to the relevant Replacement Supplier or Replacement Sub-contractor (as the case may be) acting in accordance with the provisions of Paragraphs 2.5 to 2.7, and in accordance with all applicable proper employment procedures set out in applicable Law, the Supplier shall indemnify the Replacement Supplier or Replacement Sub-contractor (as the case may be) against all Employee Liabilities arising out of the termination of employment pursuant to the provisions of Paragraph 2.7, provided that the relevant Replacement Supplier takes, or (as appropriate) procures that the relevant Replacement Sub-contractor takes, all reasonable steps to minimise any such Employee Liabilities.

2.9 The indemnity in Paragraph 2.8:

(a) shall not apply to:

(i) any claim for:

- (A) discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage, civil partnership, pregnancy, maternity, sexual orientation, religion or belief; or
- (B) equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees,

in any case in relation to any alleged act or omission of any Replacement Supplier or Replacement Sub-contractor; or

(ii) any claim that the termination of employment was unfair because the Replacement Supplier or Replacement Sub-contractor neglected to follow a fair dismissal procedure; and

(b) shall apply only where the notification referred to in Paragraph 2.5(a) is made by the relevant Replacement Supplier or Replacement Sub-contractor (as the case may be) to the Supplier within 6 months of the Service Transfer Date.

2.10 If any such person as is described in Paragraph 2.5 is neither re-employed by the Supplier or any Sub-contractor nor dismissed by the relevant Replacement Supplier or Replacement Sub-contractor within the time scales set out in Paragraphs 2.5 to 2.7, such person shall be treated as a Transferring Supplier Employee.

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 2.11 The Supplier shall, and shall procure that each Sub-contractor shall, promptly provide to the Authority, any Replacement Supplier and any Replacement Sub-contractor in writing such information as is necessary to enable the Authority, the Replacement Supplier and Replacement Sub-contractor to carry out their respective duties under regulation 13 of the Employment Regulations. The Authority shall procure that any Replacement Supplier and any Replacement Sub-contractor shall promptly provide to the Supplier and each Sub-contractor in writing such information as is necessary to enable the Supplier and each Sub-contractor to carry out their respective duties under regulation 13 of the Employment Regulations.
- 2.12 Subject to Paragraph 2.13, the Authority shall procure that any Replacement Supplier indemnifies the Supplier on its own behalf and on behalf of any Replacement Sub-contractor against any Employee Liabilities arising from or as a result of:
- (a) any act or omission of the Replacement Supplier or Replacement Sub-contractor in respect of any Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List or any appropriate representative (as defined in the Employment Regulations) of any such Transferring Supplier Employee;
 - (b) the breach or non-observance by the Replacement Supplier or Replacement Sub-contractor on or after the Service Transfer Date of:
 - (i) any collective agreement applicable to the Transferring Supplier Employees identified in the Supplier's Final Supplier Personnel List; or
 - (ii) any custom or practice in respect of any Transferring Supplier Employees identified in the Supplier's Final Supplier Personnel List which the Replacement Supplier or Replacement Sub-contractor is contractually bound to honour;
 - (c) any claim by any trade union or other body or person representing any Transferring Supplier Employees identified in the Supplier's Final Supplier Personnel List arising from or connected with any failure by the Replacement Supplier or Replacement Sub-contractor to comply with any legal obligation to such trade union, body or person arising on or after the Service Transfer Date;
 - (d) any proposal by the Replacement Supplier or Replacement Sub-contractor to change the terms and conditions of employment or working conditions of any Transferring Supplier Employees identified in the Supplier's Final Supplier Personnel List on or after their transfer to the Replacement Supplier or Replacement Sub-contractor (as the case may be) on the Service Transfer Date, or to change the terms and conditions of employment or working conditions of any person identified in the Supplier's Final Supplier

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Personnel List who would have been a Transferring Supplier Employee but for their resignation (or decision to treat their employment as terminated under regulation 4(9) of the Employment Regulations) before the Service Transfer Date as a result of or for a reason connected to such proposed changes;

- (e) any statement communicated by the Replacement Supplier or Replacement Sub-contractor to, or action undertaken by the Replacement Supplier or Replacement Sub-contractor in respect of, any Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List on or before the Service Transfer Date regarding the Relevant Transfer which has not been agreed in advance with the Supplier in writing;
- (f) any proceeding, claim or demand by HMRC or any other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:
 - (i) in relation to any Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List, to the extent that the proceeding, claim or demand by HMRC or such other statutory authority relates to financial obligations arising on and after the Service Transfer Date; and
 - (ii) in relation to any employee who is not a Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List, and in respect of whom it is later alleged or determined that the Employment Regulations applied so as to transfer their employment from the Supplier or Sub-contractor to the Replacement Supplier or Replacement Sub-contractor to the extent that the proceeding, claim or demand by HMRC or such other statutory authority relates to financial obligations arising on and after the Service Transfer Date;
- (g) a failure of the Replacement Supplier or Replacement Sub-contractor to discharge or procure the discharge of all wages, salaries, other benefits, PAYE tax deductions and national insurance contributions relating to the Transferring Supplier Employees identified in the Supplier's Final Supplier Personnel List in respect of the period on and after the Service Transfer Date; and
- (h) any claim made by or in respect of a Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List or any appropriate representative (as defined in the Employment Regulations) of any such Transferring Supplier Employee relating to any act or omission of the Replacement Supplier or Replacement Sub-contractor in relation to obligations under regulation 13 of the Employment Regulations.

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 2.13 The indemnities in Paragraph 2.12 shall not apply to the extent that the Employee Liabilities arise or are attributable to any act or omission of the Supplier or any Sub-contractor whether occurring or having its origin before, on or after the Service Transfer Date, including any Employee Liabilities arising from the failure by the Supplier or any Sub-contractor to comply with its obligations under the Employment Regulations.

SCHEDULE 28 (STAFF TRANSFER)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX E1: LIST OF NOTIFIED SUB-CONTRACTORS

SCHEDULE 28 (STAFF TRANSFER)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX E2: STAFFING INFORMATION

EMPLOYEE INFORMATION (ANONYMISED)

Name of Transferor:

Number of Employees in-scope to transfer:

Completion notes

- 1 If you have any Key Sub-contractors, please complete all the required information for any staff employed by such Key Sub-contractor(s) in a separate spreadsheet.
- 2 This spreadsheet is used to collect information from the current employer (transferor) about employees performing the relevant services to help plan for a potential TUPE transfer. Some or all of this information may be disclosed to bidders as part of a procurement process. The information should not reveal the employees' identities.
- 3 If the information cannot be included on this form, attach the additional information, such as relevant policies, and cross reference to the item number and employee number where appropriate.

EMPLOYEE DETAILS & KEY TERMS							
Details	Job Title	Grade / band	Work Location	Date of Birth (dd/mm/yy)	Employment status (for example, employee, fixed-term employee, self-employed, agency worker)?	Continuous service date (dd/mm/yy)	Date employment started with existing employer
Emp No 1							
Emp No 2							
Emp No							
Emp No							
Emp No							
Emp No							
Emp No							

EMPLOYEE DETAILS & KEY TERMS							
Details	Contract end date (if fixed term contract or temporary contract)	Contractual notice period	Contractual weekly hours	Regular overtime hours per week	Mobility or flexibility clause in contract?	Previously TUPE transferred to organisation? If so, please specify (i) date of transfer, (ii) name of transferor, and (iii) whether ex public sector	Any collective agreements?
Emp No 1							
Emp No 2							
Emp No							
Emp No							
Emp No							
Emp No							

	ASSIGNMENT	CONTRACTUAL PAY AND BENEFITS						
Details	% of working time dedicated to the provision of services under the contract	Salary (or hourly rate of pay)	Payment interval (weekly / fortnightly / monthly)	Bonus payment for previous 12 months (please specify whether contractual or discretionary entitlement)	Pay review method	Frequency of pay reviews	Agreed pay increases	Next pay review date
Emp No 1								
Emp No 2								
Emp No								
Emp No								
Emp No								
Emp No								

CONTRACTUAL PAY AND BENEFITS								
Details	Any existing or future commitment to training that has a time-off or financial implication	Car allowance (£ per year)	Lease or company car details	Any other allowances paid (e.g. shift allowance, standby allowance, travel allowance)	Private medical insurance (please specify whether single or family cover)	Life assurance (xSalary)	Long Term Disability / PHI (% of Salary)	Any other benefits in kind
Emp No 1								
Emp No 2								
Emp No								
Emp No								
Emp No								
Emp No								
Emp No								

CONTRACTUAL PAY AND BENEFITS						
Details	Annual leave entitlement (excluding bank holidays)	Bank holiday entitlement	Method of calculating holiday pay (i.e. based on fixed salary only or incl. entitlements to variable remuneration such as bonuses, allowances, commission or overtime pay?)	Maternity or paternity or shared parental leave entitlement and pay	Sick leave entitlement and pay	Redundancy pay entitlement (statutory / enhanced / contractual / discretionary)
Emp No 1						
Emp No 2						
Emp No						
Emp No						
Emp No						
Emp No						
Emp No						

PENSIONS						
Details	Employee pension contribution rate	Employer pension contribution rate	Please provide the name of the pension scheme and a link to the pension scheme website	Is the scheme an occupational pension scheme as defined in the Pension Schemes Act 1993?	If the scheme is not an occupational pension scheme, what type of scheme is it? E.g. personal pension scheme?	Type of pension provision e.g. defined benefit (CARE or final salary, and whether a public sector scheme e.g. CSPA, NHSPA, LGPS etc. or a broadly comparable scheme) or a defined contribution scheme or an auto enrolment master trust?
Emp No 1						
Emp No 2						
Emp No						
Emp No						
Emp No						
Emp No						
Emp No						

PENSIONS						
Details	If the Employee is in the Local Government Pension Scheme, please supply details of Fund and Administering Authority.	If the Employee is in the Civil Service Pension Scheme, please provide details of the Admission Agreement.	If the Employee is in the NHSPS, please provide details of the Direction Letter.	If the Employee is in a broadly comparable pension scheme, please supply a copy of the GAD certificate of Broad Comparability.	Did Fair Deal or any other similar pension protection for ex-public sector employees apply to the employee when they TUPE transferred into your employment? If so, what was the nature of that protection (e.g. right to participate in a public sector pension scheme, or a broadly comparable scheme, or to bulk transfer past pension service into their current scheme)?	If Fair Deal, Best Value or other pension protection applied, which public sector employer did they originally transfer out of and when?
Emp No 1						
Emp No 2						
Emp No						
Emp No						
Emp No						
Emp No						
Emp No						

	OTHER		
Details	Security Check Level	Security Clearance Expiry date	Additional info or comments
Emp No 1			
Emp No 2			
Emp No			
Emp No			
Emp No			
Emp No			
Emp No			

SCHEDULE 29 (KEY PERSONNEL)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SCHEDULE 29

KEY PERSONNEL

SCHEDULE 29 (KEY PERSONNEL)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Schedule 29 (*Key Personnel*)

1. This Schedule lists the key roles (“**Key Roles**”) and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date (“**Key Personnel**”).

Key Role	Name of Key Personnel	Responsibilities	Phase of the Services during which they will be a member of Key Personnel

[REDACTED]			

SCHEDULE 29 (KEY PERSONNEL)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Key Role	Name of Key Personnel	Responsibilities	Phase of the Services during which they will be a member of Key Personnel

[REDACTED]			

SCHEDULE 29 (KEY PERSONNEL)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Key Role	Name of Key Personnel	Responsibilities	Phase of the Services during which they will be a member of Key Personnel

[REDACTED]			

SCHEDULE 29 (KEY PERSONNEL)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Key Role	Name of Key Personnel	Responsibilities	Phase of the Services during which they will be a member of Key Personnel

[REDACTED]			

SCHEDULE 29 (KEY PERSONNEL)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Key Role	Name of Key Personnel	Responsibilities	Phase of the Services during which they will be a member of Key Personnel

[REDACTED]			

SCHEDULE 30 (DEED OF GUARANTEE)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 30

DEED OF GUARANTEE

SCHEDULE 30 (DEED OF GUARANTEE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Schedule 30 (*Deed of Guarantee*)

Note: The Authority does not require the Guarantee to be entered into at the Effective Date.

[Insert the name of the Guarantor]

- and -

[Insert the name of the Beneficiary]

DEED OF GUARANTEE

THIS DEED is executed as a deed and dated [Insert date of execution] (the “**Deed**”)

BETWEEN:

- (1) **[INSERT NAME OF THE GUARANTOR]** [a company incorporated in [England and Wales] under registered number [insert registered number] whose registered office is at [insert registered office]] **[OR]** [a company incorporated under the laws of [insert country], registered in [insert country] with number [insert number] at [insert place of registration], whose principal office is at [insert office details] (the “**Guarantor**”); and
- (2) **[INSERT NAME OF THE AUTHORITY]**, [acting on behalf of the Crown] of [insert the Authority’s address] (the “**Authority**”).

together the “**Parties**” and each a “**Party**”.

BACKGROUND:

- (A) The Authority [has awarded] a contract dated [insert date] to [insert details of the Supplier] (the “**Supplier**”) for the provision of [insert details of goods or services to be provided] (the “**Guaranteed Agreement**”).
- (B) It is a condition of the Authority entering into the Guaranteed Agreement that the Supplier procures the execution and delivery to the Authority of a parent company guarantee substantially in the form of this Deed.
- (C) The Guarantor has agreed to guarantee the due performance of the Guaranteed Agreement.

IT IS AGREED as follows:

1 DEFINITIONS AND INTERPRETATION

Definitions

- 1.1 The **following** definitions apply in this Deed:

SCHEDULE 30 (DEED OF GUARANTEE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

"Business Day"	means a day, other than a Saturday, Sunday or public holiday in England, when banks in London are open for business;
"Control"	means the power of a person to secure that the affairs of a body corporate are conducted in accordance with the wishes of that person: (a) by means of the holding of shares or the possession of voting power in relation to that body or any other body corporate; or (b) as a result of any powers conferred by the constitutional or corporate documents, or any other document regulating that body or any other body corporate;
"Guaranteed Agreement"	has the meaning given to it in Recital (A);
"Guaranteed Obligations"	has the meaning given to it in Clause 2.1(a);
"Supplier"	has the meaning given to it in Recital (A);
"VAT"	means value added tax or any equivalent tax chargeable in the UK or elsewhere.

Interpretation

1.2 Unless otherwise stated, any reference in this Deed to:

- (a) the "Guarantor", the "Authority", the "Supplier" or any other person shall be construed so as to include their successors in title, permitted assigns and permitted transferees, whether direct or indirect;
- (b) "assets" includes present and future properties, revenues and rights of every description;
- (c) this "Deed", or any other agreement or instrument is a reference to, this deed or other agreement or instrument as amended, novated, supplemented, extended or restated;
- (d) "indebtedness" includes any obligation (whether incurred as principal or as surety) for the payment or repayment of money, whether present or future, actual or contingent;

SCHEDULE 30 (DEED OF GUARANTEE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (e) a "person" includes any individual, firm, company, corporation, government, state or agency of a state or any association, trust, joint venture, consortium, partnership or other entity (whether or not having separate legal personality);
- (f) the words "including", "includes", "in particular", "for example" or similar shall be construed as illustrative and without limitation to the generality of the related general words; and
- (g) a time of day is a reference to London time.

2 GUARANTEE AND INDEMNITY**2.1 The Guarantor:**

- (a) guarantees to the Authority the due and punctual performance of all of the Supplier's present and future obligations under and in connection with the Guaranteed Agreement if and when they become due and performable in accordance with the terms of the Guaranteed Agreement (the "**Guaranteed Obligations**");
- (b) shall pay to the Authority from time to time on demand all monies (together with interest on such sum accrued before and after the date of demand until the date of payment) that have become payable by the Supplier to the Authority under or in connection with the Guaranteed Agreement but which has not been paid at the time the demand is made; and
- (c) shall, if the Supplier fails to perform in full and on time any of the Guaranteed Obligations and upon written notice from the Authority, immediately on demand perform or procure performance of the same at the Guarantor's own expense.

2.2 The Guarantor, as principal obligor and as a separate and independent obligation and liability from its obligations and liabilities under Clause 2.1, shall indemnify and keep indemnified the Authority in full and on demand from and against all and any losses, damages, costs and expenses suffered or incurred by the Authority arising out of, or in connection with:

- (a) any failure by the Supplier to perform or discharge the Guaranteed Obligations; or
- (b) any of the Guaranteed Obligations being or becoming wholly or partially unenforceable for any reason,
- (c) provided that the Guarantor's liability under this Clause 2.2 shall be no greater than the Supplier's liability under the Guaranteed Agreement was (or would have been had the relevant Guaranteed Obligation been fully enforceable).

3 AUTHORITY PROTECTIONS

SCHEDULE 30 (DEED OF GUARANTEE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Continuing Guarantee

- 3.1 This Deed is, and shall at all times be, a continuing and irrevocable security until the Guaranteed Obligations have been satisfied or performed in full, and is in addition to and not in substitution for and shall not merge with any other right, remedy, guarantee or security which the Authority may at any time hold for the performance of the Guaranteed Obligations and may be enforced without first having recourse to any such security.

Preservation of the Guarantor's liability

- 3.2 The Guarantor's liability under this Deed shall not be reduced, discharged or otherwise adversely affected by:
- (a) any arrangement made between the Supplier and the Authority;
 - (b) any partial performance (except to the extent of such partial performance) by the Supplier of the Guaranteed Obligations;
 - (c) any alteration in the obligations undertaken by the Supplier whether by way of any variation referred to in Clause 4 or otherwise;
 - (d) any waiver or forbearance by the Authority whether as to payment, time, performance or otherwise;
 - (e) the taking, variation, renewal or release of, the enforcement or neglect to perfect or enforce any right, guarantee, remedy or security from or against the Supplier or any other person;
 - (f) any unenforceability, illegality or invalidity of any of the provisions of the Guaranteed Agreement or any of the Supplier's obligations under the Guaranteed Agreement, so that this Deed shall be construed as if there were no such unenforceability, illegality or invalidity;
 - (g) any dissolution, amalgamation, reconstruction, reorganisation, change in status, function, Control or ownership, insolvency, liquidation, administration, voluntary arrangement, or appointment of a receiver, of the Supplier or any other person.

Immediate demand

- 3.3 The Guarantor waives any right it may have to require the Authority to proceed against, enforce any other right or claim for payment against, or take any other action against, the Supplier or any other person before claiming from the Guarantor under this Guarantee.

Deferral of rights

- 3.4 Until all amounts which may be or become payable under the Guaranteed Agreement or this Deed have been irrevocably paid in full, the Guarantor shall not, as a result of this Deed or any payment performance under this Deed:

SCHEDULE 30 (DEED OF GUARANTEE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (a) be subrogated to any right or security of the Authority;
- (b) claim or prove in competition with the Authority against the Supplier or any other person;
- (c) demand or accept repayment in whole or in part of any indebtedness due from the Supplier;
- (d) take the benefit of, share in or enforce any security or other guarantee or indemnity against the Supplier; or
- (e) claim any right of contribution, set-off or indemnity from the Supplier,

without the prior written consent of the Authority (and in such case only in accordance with any written instructions of the Authority).

- 3.5 If the Guarantor receives any payment or other benefit in breach of Clause 3.4, or as a result of any action taken in accordance with a written instruction of the Authority given pursuant to Clause 3.4, such payment or other benefit, and any benefit derived directly or indirectly by the Guarantor therefrom, shall be held by the Guarantor on trust for the Authority applied towards the discharge of the Guarantor's obligations to the Authority under this Deed.

4 VARIATION OF THE GUARANTEED AGREEMENT

- 4.1 The Guarantor confirms that it intends that this Deed shall extend and apply from time to time to any variation, increase, extension or addition of the Guaranteed Agreement, however, fundamental, and any associated fees, costs and/or expenses.

5 PAYMENT AND COSTS

- 5.1 All sums payable by the Guarantor under this Deed shall be paid in full to the Authority in pounds sterling:
- (a) without any set-off, condition or counterclaim whatsoever; and
 - (b) free and clear of any deductions or withholdings whatsoever except as may be required by applicable law which is binding on the Guarantor.
- 5.2 If any deduction or withholding is required by any applicable law to be made by the Guarantor:
- (a) the amount of the payment due from the Guarantor shall be increased to an amount which (after making any deduction or withholding) leaves an amount equal to the payment which would have been due if no deduction or withholding had been required; and

SCHEDULE 30 (DEED OF GUARANTEE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) the Guarantor shall promptly deliver to the Authority all receipts issued to it evidencing each deduction or withholding which it has made.
- 5.3 The Guarantor shall not and may not direct the application by the Authority of any sums received by the Authority from the Guarantor under any of the terms in this Deed.
- 5.4 The Guarantor shall pay interest on any amount due under this Deed at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgment.
- 5.5 The Guarantor shall, on a full indemnity basis, pay to the Authority on demand the amount of all costs and expenses (including legal and out-of-pocket expenses and any VAT on those costs and expenses) which the Authority incurs in connection with:
 - (a) the preservation, or exercise and enforcement, of any rights under or in connection with this Deed or any attempt to do so; and
 - (b) any discharge or release of this Deed.

6 CONDITIONAL DISCHARGE

- 6.1 Any release, discharge or settlement between the Guarantor and the Authority in relation to this Deed shall be conditional on no right, security, disposition or payment to the Authority by the Guarantor, the Supplier or any other person being avoided, set aside or ordered to be refunded pursuant to any enactment or law relating to breach of duty by any person, bankruptcy, liquidation, administration, protection from creditors generally or insolvency for any other reason.
- 6.2 If any such right, security, disposition or payment as referred to in Clause 6.1 is avoided, set aside or ordered to be refunded, the Authority shall be entitled subsequently to enforce this Deed against the Guarantor as if such release, discharge or settlement had not occurred and any such security, disposition or payment has not been made.

7 REPRESENTATIONS AND WARRANTIES

- 7.1 The Guarantor represents and warrants to the Authority that:
 - (a) it is duly incorporated with limited liability and is a validly existing company under the laws of its place of incorporation, has the capacity to sue or be sued in its own name, and has power to carry on its business as now being conducted and to own its property and other assets;

SCHEDULE 30 (DEED OF GUARANTEE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) it has full power under its constitution or equivalent constitutional documents in the jurisdiction in which it is established to enter into this Deed;
- (c) it has full power to perform the obligations expressed to be assumed by it or contemplated by this Deed;
- (d) it has been duly authorised to enter into this Deed;
- (e) it has taken all necessary corporate action to authorise the execution, delivery and performance of this Deed;
- (f) this Deed when executed and delivered will constitute a legally binding obligation on it enforceable in accordance with its terms;
- (g) all necessary consents and authorisations for the giving and implementation of this Deed have been obtained;
- (h) that its entry into and performance of its obligations under this Deed will not constitute any breach of or default under any contractual, government or public obligation binding on it; and
- (i) that it is not engaged in any litigation or arbitration proceedings that might affect its capacity or ability to perform its obligations under this Deed and to the best of its knowledge no such legal or arbitration proceedings have been threatened or are pending against it.

8 ASSIGNMENT

- 8.1 The Authority shall be entitled by notice in writing to the Guarantor to assign the benefit of this Deed at any time to any person without the consent of the Guarantor being required and any such assignment shall not release the Guarantor from liability under this Deed.
- 8.2 The Guarantor may not assign or transfer any of its rights and/or obligations under this Deed without the prior written consent of the Authority.

9 VARIATION

- 9.1 No variation of this Deed shall be effective unless it is in writing and signed by the parties.

10 DEMANDS AND NOTICES

- 10.1 Any demand or notice served by the Authority on the Guarantor under this Deed shall be in writing, addressed to:
 - (a) For the Attention of [insert details]
 - (b) [Address of the Guarantor in England and Wales]

SCHEDULE 30 (DEED OF GUARANTEE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 10.2 or such other address in England and Wales as the Guarantor has from time to time notified to the Authority in writing in accordance with the terms of this Deed as being an address or facsimile number for the receipt of such demands or notices.
- 10.3 Any notice or demand served on the Guarantor or the Authority under this Deed shall be deemed to have been served:
- (a) if delivered by hand, at the time of delivery; or
 - (b) if posted, at 10.00 a.m. on the second Business Day after it was put into the post.
- 10.4 In proving service of a notice or demand on the Guarantor it shall be sufficient to prove that delivery was made, or that the envelope containing the notice or demand was properly addressed and posted as a prepaid first class recorded delivery letter.
- 10.5 Any notice purported to be served on the Authority under this Deed shall only be valid when received in writing by the Authority.

11 ENTIRE AGREEMENT

- 11.1 This Deed constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.
- 11.2 The Guarantor acknowledges that it has not entered into this Deed in reliance upon, nor has it been induced to enter into this Deed by, any representation, warranty or undertaking made by or on behalf of the Authority (whether express or implied and whether pursuant to statute or otherwise) which is not set out in this Deed.

12 WAIVER

- 12.1 No failure or delay by the Authority to exercise any right or remedy provided under this Deed or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.
- 12.2 Any waiver by the Authority of any terms of this Deed, or of any Guaranteed Obligations, shall only be effective if given in writing and then only for the purpose and upon the terms and conditions, if any, on which it is given.

13 SEVERANCE

- 13.1 If any provision or part-provision of this Deed is or becomes invalid, illegal or unenforceable for any reason, such provision or part-provision shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this Deed.

SCHEDULE 30 (DEED OF GUARANTEE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

14 THIRD PARTY RIGHTS

- 14.1 A person who is not a Party to this Deed shall have no right under the Contracts (Rights of Third Parties) Act 1999 (as amended, updated or replaced from time to time) to enforce any of its terms but this does not affect any third party right which exists or is available independently of that Act.

15 GOVERNING LAW AND JURISDICTION

- 15.1 This Deed and any issues, disputes or claims (whether contractual or non-contractual) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws of England and Wales.
- 15.2 The Guarantor irrevocably agrees for the benefit of the Authority that the courts of England shall have jurisdiction to settle any dispute or claim (whether contractual or non-contractual) that arises out of or in connection with this Deed or its subject matter or formation.
- 15.3 Nothing contained in Clause 15.2 shall limit the rights of the Authority to take proceedings against the Guarantor in any other court of competent jurisdiction, nor shall the taking of any such proceedings in one or more jurisdictions preclude the taking of proceedings in any other jurisdiction, whether concurrently or not (unless precluded by applicable law).
- 15.4 The Guarantor irrevocably waives any objection which it may have now or in the future to the courts of England being nominated for the purpose of this Clause on the ground of venue or otherwise and agrees not to claim that any such court is not a convenient or appropriate forum.
- 15.5 [The Guarantor irrevocably appoints [Insert name of agent] of [Insert address of agent] as its agent to receive on its behalf in England or Wales service of any proceedings under this Clause 15. Such service shall be deemed completed on delivery to such agent (whether or not it is forwarded to and received by the Guarantor) and shall be valid until such time as the Authority has received prior written notice that such agent has ceased to act as agent. If for any reason such agent ceases to be able to act as agent or no longer has an address in England or Wales, the Guarantor shall appoint a substitute acceptable to the Authority and deliver to the Authority the new agent's name and address within England and Wales.]

SCHEDULE 30 (DEED OF GUARANTEE)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Executed as a deed by [insert the name of the Guarantor] acting by [insert name of Director] a director, in the presence of a witness:

.....
[Signature of Witness]

.....
[Signature of Director]

Name of Director:

.....

Name of Witness:

.....

Address of Witness:

.....

.....

Occupation of Witness:

.....

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 31

PROCESSING PERSONAL DATA

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 31 (*Processing Personal Data*)

- 1.1 This Schedule shall be completed by the Controller, who may take account of the view of the Processor, however the final decision as to the content of this Schedule shall be with the Authority at its absolute discretion.
- 1.2 The contact details of the Authority's Data Protection Officer are: dataprotection@justice.gov.uk
- 1.3 The contact details of the Supplier's Data Protection Officer are: Data.protection@vodafone.com
- 1.4 The Processor shall comply with any further written instructions with respect to processing by the Controller.
- 1.5 Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of Controller for each Category of Personal Data	The Parties are Independent Controllers of Personal Data The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: • Business contact details of Supplier Personnel, • Business contact details of any directors, officers, employees, agents, consultants and contractors of the Authority (excluding the Supplier Personnel) engaged in the performance of the Authority's duties under this Contract. • Where the Supplier has professional or regulatory obligations in respect of the Personal Data received. • For billing and contract administration including personal data that is processed incidentally in providing the services. • A standardised service is such that the Authority cannot dictate the way in which Personal Data is processed by the Supplier. • Where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Authority.
Subject matter of the Processing	Processing for the provision of the Contract to provide Services as described in the Contract and Schedule 2 (Services Description) specifically.
Duration of the processing	The Term and (to the extent relevant) the Termination Assistance Period.

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Scope, Nature and purposes of the processing	Scope of the Processing: Processing shall include: • Processing as necessary for delivery of the Services (the “Controller Services”) including: - Provisioning of WAN Connectivity at Authority Sites and – if applicable for some broadband connections – at home addresses of End Users (e.g. senior justices); - Configuration and management of the IT Environment (e.g. as required for Gateway Services and/or Core Network Services); - Service management, including use of and/or integration with the ITSM Toolset; - Device handling (e.g. where personal data may be recoverable from Devices); - Creating employment and training opportunities, including selection and management of candidates from HM Prison and Probation Service as required under the Social Value Delivery Plan. Nature of the Processing: The nature of the processing is as set out in relevant provisions of the Contract, including but not limited to: collection, recording, organisation, structuring, storage, analysis, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or, restriction, erasure or destruction of data (whether or not by automated means) and any other Processing activity to deliver the Controller Services. Purpose of the Processing: The purpose of the processing is to provide and operate the Controller Services.
Type of Personal Data	Personal data including: • Business contact information (e.g. names, business address, e-mail address) • Home address information (e.g. for broadband lines) • User authentication data (e.g. usernames; credentials) • Device hostnames and nicknames • Access logs • Service management records (e.g. relating to Incidents, requests for change) • Device/user metadata (e.g. IP addresses; MAC addresses) where such data relates to an identified or identifiable End User.

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

	• Employment/training candidates' prison records including any training programmes undertaken during prison term, as well as information on candidates' education and employment history, and any other personal information required under the Social Value Delivery Plan.
Categories of Data Subject	Categories of Data Subject may include: • End Users • Employees, representatives and contractors of the Authority • Supplier Personnel • Candidates for employment and training opportunities under the Social Value Delivery Plan, including prisoners, prison-leavers and people on probation • Authority's customers, employees or representatives, contractors or end-users, Supplier's employees or representatives.
Plan for return and destruction of the data once the processing is complete UNLESS requirement under law to preserve that type of data	Personal Data should not be processed for longer than necessary in accordance with paragraph 16 (Retention) of Annex 4 of this Schedule. Data retention requirements are in line with "MoJ Cyber and Technical Security Guidance" as stated in Schedule 4, paragraph 10.1
Locations at which the Supplier and/or its Sub-contractors process Personal Data under this Contract and international transfers and legal gateway	United Kingdom (subject to the below). The Authority acknowledges that it may require the Supplier to use Authority Assets in the provision of the Services. If Authority Assets are hosted outside of the UK and therefore the use of such Authority Assets by the Supplier would constitute a transfer of Personal Data outside of the UK, the Authority hereby consents to such transfer and considers that the requirements on Clause 21.6(d) are satisfied. The Authority confirms that it has in place appropriate safeguards for such transfer in accordance with Data Protection Legislation.
Protective Measures that the Supplier and, where applicable, its Sub-contractors shall have in place to protect Personal Data processed under this Contract against a breach of security (insofar as that breach of security relates to data) or a Personal Data Breach	[REDACTED] [REDACTED] [REDACTED] [REDACTED]

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference:

[illegible]

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

		[REDACTED]
		[REDACTED]

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 1: NOT USED

ANNEX 2: NOT USED

ANNEX 3: NOT USED

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 4: INDEPENDENT CONTROLLER CLAUSES

1 Definitions and interpretation

1.1 In this Schedule:

Communication

means a complaint, enquiry, notice, request or other communication (but excluding any Data Subject Request) relating to either party's obligations under any Data Protection Legislation in connection with this Contract and/or the Processing of any of the Shared Personal Data, including any compensation claim from a Data Subject or any notice, investigation or other action from a Data Protection Supervisory Authority relating to any of the foregoing;

Consent

means a freely given, specific, informed and unambiguous indication (by a statement or by a clear affirmative action) by which the relevant Data Subject has agreed to the relevant transfer(s) and/or Processing of the Shared Personal Data relating to them that has not been withdrawn. To the extent the relevant Shared Personal Data is Special Category Personal Data, this definition should be read as if the word 'unambiguous' above read 'unambiguous and explicit'. The terms **freely given**, **specific**, **informed**, **unambiguous** and **explicit** in this definition shall be construed in accordance with Data Protection Legislation;

Contact Point

means, in respect of each Party, the person identified as such in accordance with paragraph 1 of Appendix 5 of this Annex 4;

Data Protection Supervisory Authority

means any regulator, authority or body responsible for administering Data Protection Legislation;

Disclosing Party

means each party to the extent it (or any person acting on its behalf) discloses or

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

otherwise makes accessible any Shared Personal Data to the other party (or any person acting on the other party's behalf);

Permitted Lawful Basis

- (a) the permitted lawful basis under Article 6(1) of the UK GDPR under which the Shared Personal Data is processed by the Authority and shared by the Authority with the Supplier, is Article 6(1)(e) of the UK GDPR – processing is necessary for the performance of a task carried out in the public interest; and
- (b) the permitted lawful basis under Article 6(1) of the UK GDPR under which the Shared Personal Data is processed by the Supplier and shared by the Supplier with the Authority, is Article 6(1)(b) of the UK GDPR – processing is necessary for the performance of a contract to which the data subject is party; and Article 6(1)(f) of the UK GDPR - processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject;

Permitted Purpose

means the Supplier shall use the Shared Personal Data for the purpose of providing the Services only;

Permitted Recipients

means the following who need access to the Received Personal Data for the Permitted Purpose:

- (a) the Supplier's employees and employees of Sub-contractors;

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

(b) the Authority's employees, contractors and advisors;

Personal Data

has the meaning given in Data Protection Legislation;

Personal Data Breach

has the meaning given in Data Protection Legislation;

Processing

has the meaning given in Data Protection Legislation (and related expressions, including **Process**, **Processed** and **Processes** shall be construed accordingly);

Received Personal Data

means Shared Personal Data in respect of which the relevant party is the Receiving Party;

Receiving Party

means each party to the extent it (or any person acting on its behalf) receives or accesses any Shared Personal Data disclosed or made available by the other party (or any person acting on the other party's behalf);

Shared Personal Data

means the Personal Data described in the table following paragraph 1.5 of this Schedule; and

Special Category Personal Data

means the categories of Personal Data set out in Article 9(1) of the UK GDPR.

2 Status of the Parties

- 2.1 Each Party shall be a Controller of the Shared Personal Data. If the Parties share the Shared Personal Data, it shall be shared and managed in accordance with the terms of this Contract.

3 Compliance with Data Protection Legislation

- 3.1 Subject to compliance by the other Party with its express obligations in other provisions of this Contract, each Party shall at all times comply with all Data Protection Legislation in connection with the exercise and performance of its respective rights and obligations under this Contract.

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 3.2 This Schedule allocates certain rights and responsibilities among the Parties as enforceable contractual obligations between themselves, however nothing in this Schedule is intended to limit or exclude either Party's responsibilities or liabilities under Data Protection Legislation.

4 Agreed basis for sharing

- 4.1 The Parties have determined that it is necessary to share the Shared Personal Data in order to achieve the Permitted Purpose.
- 4.2 The Parties agree that this Schedule relates to ongoing and routine data sharing.
- 4.3 The Parties have documented additional details relating to the sharing of the Shared Personal Data in Appendix 2 of this Annex 4, which includes:
- 4.3.1 the aims of each Party in sharing the Shared Personal Data;
 - 4.3.2 why sharing the Shared Personal Data on the terms of this Schedule is necessary to achieve those aims; and
 - 4.3.3 the benefits to the Data Subjects and/or society of the Parties sharing the Shared Personal Data.

5 General obligations

- 5.1 Each Party, to the extent it acts as Receiving Party, undertakes to the relevant Disclosing Party that it shall undertake all Processing of Received Personal Data only:
- 5.1.1 for the Permitted Purpose in accordance with this Schedule and in all respects in accordance with Data Protection Legislation; and
 - 5.1.2 to the extent consistent with the Permitted Lawful Basis, except to the extent otherwise required by Law.
- 5.2 The Parties agree that in respect of Shared Personal Data, the relevant Disclosing Party:
- 5.2.1 is, as between the Parties and subject to paragraphs 5.3 and 9.1, the primary point of contact for Data Subjects;
 - 5.2.2 subject to paragraphs 5.3 and 9.1, shall direct Data Subjects to its Contact Point in connection with the exercise of their rights as Data Subjects and for any enquiries concerning the Shared Personal Data

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

and identify its Contact Point in all information referred to in paragraphs 5.2.5 and 5.3 as the contact point for all Data Subject Requests or other Communications from Data Subjects regarding the sharing or other Processing of such Shared Personal Data;

- 5.2.3 shall ensure that the Shared Personal Data has been collected, Processed and transferred in accordance with the Data Protection Legislation as applicable to that data at all times prior to the receipt of that data by the Receiving Party (or any person acting on its behalf);
- 5.2.4 shall ensure the Shared Personal Data is accurate and up-to-date when disclosed or made accessible to the relevant Receiving Party and shall promptly notify the Receiving Party if such Shared Personal Data becomes inaccurate or out of date during the Term (together with revised and corrected data);
- 5.2.5 is solely responsible for both Parties' compliance with all duties to provide information to Data Subjects under Articles 5(1)(a), 13 and 14 of the UK GDPR or any similar Data Protection Legislation, including as required for all Processing of Shared Personal Data by or on behalf of the Receiving Party for the Permitted Purpose on the Permitted Lawful Basis in accordance with this Schedule and shall comply with its respective obligations in Appendix 4 of this Annex 4;
- 5.2.6 shall ensure that the Shared Personal Data when transferred to the Receiving Party (or anyone acting on its behalf) in connection with this Contract:
- (a) is not subject (or potentially subject) to any laws giving effect to Article 71 (Protection of personal data) of the agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community; and
 - (b) is not subject to the laws of any jurisdiction outside of the United Kingdom;
- 5.2.7 without prejudice to its other obligations, shall ensure that it is entitled to transfer the Shared Personal Data to the Receiving Party and that the Receiving Party (and each of the Receiving Party's Permitted Recipients) is entitled under all applicable laws and legal theories to Process the Shared Personal Data for the Permitted Purpose in accordance with the terms of this Contract;

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

5.2.8 shall promptly notify the Receiving Party if a relevant Data Subject has requested that their Shared Personal Data is no longer Processed by either Party for the Permitted Purpose;

5.2.9 is solely responsible for ensuring that where the Shared Personal Data was received by the Disclosing Party from a third party, or has been Processed by a third party on behalf of the Disclosing Party, it has in place arrangements with those third parties:

- (a) as required by all Data Protection Legislation (including, where applicable, Articles 26, 28 and 32 of the UK GDPR);
- (b) which are adequate to permit the Disclosing Party to share the Shared Personal Data with the Receiving Party (and its Permitted Recipients) under all Data Protection Legislation; and
- (c) as required for the Receiving Party (and its Permitted Recipients) to Process such data in accordance with this Contract.

5.3 Notwithstanding the terms of this Contract, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation against any relevant party as Controller.

5.4 Each Party shall use its reasonable endeavours to assist the other to comply with any obligations under all Data Protection Legislation in connection with this Contract and shall not perform its obligations under this Contract in such a way as to cause the other Party to breach any of the other Party's obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

5.5 Without prejudice to any other obligation, if either Party becomes aware any of the Shared Personal Data is inaccurate or out of date, it shall promptly notify the other.

6 Technical and organisational measures

6.1 The Receiving Party shall at all times:

6.1.1 put in place and maintain appropriate technical and organisational measures as required by Data Protection Legislation;

6.1.2 implement and maintain appropriate technical and organisational measures to protect the Received Personal Data in its possession or control against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access, taking into account:

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (a) the nature of the data to be protected;
 - (b) the harm that might result from any failure to so protect the Received Personal Data;
 - (c) the state of technological development; and
 - (d) the cost of implementing any measures;
- 6.1.3 ensure that it has the capability (technological and otherwise), to the extent required by Data Protection Legislation, to:
 - (a) provide, correct or delete at the request of a Data Subject all the Received Personal Data relating to that Data Subject; and
 - (b) comply with any Data Subject Requests; and
- 6.1.4 without prejudice to any other obligation in this paragraph 6, implement and comply with the technical and organisational measures specified in Appendix 3 of this Annex 4.
- 6.2 Each Party shall comply with its respective obligations, and may exercise its respective rights and remedies, under Appendix 3 of this Annex 4.

7 Third party Processing

- 7.1 Each Party undertakes not to disclose or transfer Received Personal Data in respect of which it is the Receiving Party to any third party other than to a Permitted Recipient where necessary for the Permitted Purpose. Each Party transferring or disclosing Received Personal Data in respect of which it is the Receiving Party shall ensure it is transferred and disclosed subject to equivalent and legally binding obligations which are no less onerous than those applicable to the Receiving Party under this Contract. This paragraph 7.1 is without prejudice to any disclosure or transfer required by Law.
- 7.2 In respect of any Processing of Received Personal Data performed by a Processor on behalf of a Receiving Party, that Receiving Party shall:
 - 7.2.1 carry out adequate due diligence on such Processor to ensure that it is capable of providing the level of protection for the Received Personal Data as is required by this Agreement and Data Protection Legislation, and provide evidence of such due diligence to the other party where reasonably requested; and
 - 7.2.2 ensure that suitable written agreements are at all times in place with each Processor as required under all Data Protection Legislation (including Articles 28 and 32 of the UK GDPR).
- 7.3 The relevant Receiving Party shall be liable to the Disclosing Party for all acts and omissions of each of its Permitted Recipients in connection with

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Received Personal Data. Each obligation in this Contract on a Party to do, or refrain from doing, any thing shall include an obligation on that Party to ensure all its Permitted Recipients do, or refrain from doing, such thing.

8 International transfers

8.1 The Receiving Party shall not transfer Received Personal Data to any country or territory outside the United Kingdom or to any international organisation (as defined in the UK GDPR), except to the extent required by Law or with the Disclosing Party's express prior written consent. For the purposes of this paragraph 8 '**transfer**' bears the same meaning as the word 'transfer' in Article 44 of the UK GDPR.

8.2 The Authority acknowledges that it may require the Supplier to use Authority Assets in the provision of the Services. If Authority Assets are hosted outside of the UK and therefore the use of such Authority Assets by the Supplier would constitute a transfer of Received Personal Data outside of the UK, the Authority hereby consents to such transfer. The Authority confirms that it has in place appropriate safeguards for such transfer in accordance with Data Protection Legislation.

9 Dealing with Data Subject Requests and Communications

9.1 Responsibility for complying with any Data Subject Request or Communication falls on the Party which first received such Data Subject Request or Communication.

9.2 If either Party receives a Communication relating to the Shared Personal Data Processed by (or on behalf of) the other Party it shall to the extent lawful under Law:

9.2.1 promptly (and in any event within two (2) Working Days of receipt) notify the other Party; and

9.2.2 consult with the other Party in advance of giving any response, to the extent reasonably practicable.

9.3 Without prejudice to paragraph 9.1, if a party which is the Receiving Party receives a Data Subject Request it believes relates to Processing of Received Personal Data, it shall promptly (and in any event within two Working Days of receipt) notify the Contact Point of the Disclosing Party and provide them with full details (to the extent lawful under Law).

9.4 Each Party shall use all reasonable endeavours to provide the other Party with full and prompt co-operation and assistance in relation to any Data

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Subject Request or Communication made to enable the other Party to comply with the relevant timescales set out in Data Protection Legislation and to find an efficient, timely and amicable solution to any issues arising out of any Data Subject Request or Communication. Without prejudice to the generality of the foregoing, the other Party shall respond to any request for co-operation or assistance under this paragraph 9.4 within three (3) Working Days.

10 Personal Data Breaches

10.1 Each Party shall promptly (and in any event within 24 hours) notify the Disclosing Party if it suspects or becomes aware of any actual or threatened occurrence of any Personal Data Breach in respect of any Received Personal Data which it (or any person acting on its behalf) Processes as Receiving Party. In such circumstances, the relevant Receiving Party shall promptly provide (to the extent permitted by Law):

10.1.1 sufficient information as the Disclosing Party (or its advisors) reasonably requires to meet any obligations to report a Personal Data Breach under Data Protection Legislation (in a timescale which facilitates such compliance);

10.1.2 the Data Protection Supervisory Authorities investigating the Personal Data Breach with complete information as requested by those Data Protection Supervisory Authorities from time to time;

10.1.3 all reasonable assistance the Disclosing Party (or its advisors) requires, including:

- (a) co-operation with Data Protection Supervisory Authorities (including with investigations or actions to mitigate or remediate the Personal Data Breach);
- (b) making available all relevant data and records required for either party to comply with Data Protection Legislation or as otherwise reasonably required by the Disclosing Party;
- (c) taking such reasonable steps as are directed by the Disclosing Party to assist in the investigation, mitigation and remediation of a Personal Data Breach (which may include providing the Disclosing Party with physical access to any facilities affected and facilitating the interview of staff and others involved in the matter); and
- (d) co-ordination with the Disclosing Party regarding the management of public relations and public statements relating to the Personal Data Breach.

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

10.2 The Receiving Party's obligations under this paragraph 10 shall be performed at the Receiving Party's cost and expense.

11 Data protection impact assessments

11.1 Where a Party considers that:

11.1.1 a data protection impact assessment is necessary for compliance with Data Protection Law; or

11.1.2 the risks identified by any previous data protection impact assessment may have changed in respect of the sharing or other Processing activities conducted under or in connection with this Contract,

the other Party shall provide such reasonable assistance as that party may reasonably require.

11.2 The assistance referred to in paragraph 11.1 may include:

11.2.1 a systematic description of the envisaged Processing operations and Permitted Purpose of the Processing of the Shared Personal Data;

11.2.2 an assessment of the necessity and proportionality of the Processing operations;

11.2.3 an assessment of the risks to the rights and freedoms of Data Subjects;

11.2.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of the Shared Personal Data; and

11.2.5 any prior consultation with the relevant Data Protection Supervisory Authority which may be necessary.

12 Records

12.1 Each Party shall maintain complete, accurate and up to date written records of all of its Processing of the Shared Personal Data and as necessary to demonstrate its compliance with this Contract and all Data Protection Legislation.

13 Review

13.1 The Parties shall comply with and maintain, the arrangements set out in Appendix 5 of this Annex 4.

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

14 Not used**15 Audit**

15.1 Each Party shall (and shall ensure all its Permitted Recipients shall) promptly:

15.1.1 make available to the other Party such information as is reasonably required to demonstrate that Party's compliance with its obligations under this Contract;

15.1.2 not more than once in any 12 month period upon reasonable prior notice allow for, permit and contribute to audits, including inspections, by the other party (or another auditor mandated by the other Party) during normal business hours to the extent necessary to verify the audited Party's compliance with its obligations under this Contract; and

15.1.3 provide (or procure) access to all relevant systems, personnel, business premises and records for the purposes of each such audit or inspection referred to in paragraph 15.1.2 and provide (and procure) all further reasonable co-operation, access and assistance in relation to any such audit or inspection.

15.2 Each Party shall allow the other to exercise its rights at paragraph 15.1 in the period up to six years after the termination or expiry of this Contract.

15.3 When conducting audits and inspections, the relevant party conducting the audit or inspection shall comply with the other Party's reasonable directions in order to minimise disruption to the other party's business and to safeguard the confidentiality of the other party's Confidential Information. The Party subject to the audit or inspection may require any third parties conducting such audit or inspection to enter into direct confidentiality undertakings with it on terms that are substantially the same as the confidentiality obligations in this Contract.

16 Retention

16.1 Subject to paragraph 16.2 and except as required by Law, each Party shall retain the Received Personal Data in accordance with the retention periods identified for the specific element of the Shared Personal Data in accordance with the table following paragraph 1.5 of this Schedule. Where the Parties are acting as Controllers, they will not retain Personal Data for longer than is necessary to fulfil their obligations under this Contract and/or any Applicable Law.

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

16.2 Except as required by Law, the Parties shall, to the extent they are Receiving Party:

16.2.1 subject to paragraphs 16.2.2 to 16.2.3 (inclusive), Process all Received Personal Data for no longer than such Processing is necessary for the Permitted Purpose and compliant with this Contract and all Data Protection Legislation;

16.2.2 cease to Process all Received Personal Data on the earlier of termination or expiry of this Contract; and

16.2.3 without undue delay, confidentially and securely destroy or dispose of all Received Personal Data (and all copies) in its possession or control that can no longer be Processed in accordance with this Contract.

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Appendix 1

How the Shared Personal Data will be shared

NOT USED

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Appendix 2**Further details of the Personal Data sharing**

This Appendix 2 of Annex 4 is included for convenience only and shall have no legal effect, including no effect on the interpretation of this Contract.

1 Data sharing objectives

The Parties have determined the following aims and objectives of sharing the Shared Personal Data for the Permitted Purpose: The aim of the sharing is to enable the Supplier to provide the Services and without such sharing the provision of the Services would not be viable.

2 Necessity

The Parties have determined that sharing the Shared Personal Data on the terms of this Contract is necessary to achieve those aims because: The sharing of the Shared Personal data will allow the Supplier to provide wide area network (WAN) services to the Authority which supports the running of the Authority, in particular the courts, prisons, probation services and attendance centres which form part of the justice system.

3 Benefits of data sharing

The Parties have determined the following benefits will be derived by Data Subjects and/or society from sharing the Shared Personal Data: The sharing will benefit society because it will support the running of WAN services in the justice system.

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Appendix 3
Technical and organisational measures

In addition to Schedule 5 (Security Management) and any other security requirements in the Contract, the Parties shall implement the following technical and organisational measures:

1 Security management

Without prejudice to its other obligations, the parties shall implement and maintain at least the following technical and organisational security measures, actively to ensure the safety and security of the Protected Data:

- 1.1 Technical and organisational measures to ensure a level of security appropriate to the risk, normally including:
 - 1.1.1 the pseudonymisation and encryption of personal data;
 - 1.1.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - 1.1.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - 1.1.4 process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
 - 1.1.5 prompt and comprehensive maintenance of the measure to ensure currency and validity against risks.
- 1.2 The measures shall demonstrably take into account the state of the art, the costs of implementation, the consequences of impact, and the nature, scope, context and purposes of processing of Protected Data to be carried out under or in connection with this agreement, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.
- 1.3 In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, storage or transmission of personal data arising from unplanned or unmanaged activities such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
- 1.4 Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 of the UK GDPR

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

may be used as an element by which to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

- 1.5 Without prejudice to its other obligations, the Supplier shall normally implement National Cyber Security Centre SaaS security principles outlined here: SaaS security principles - NCSC.GOV.UK

2 Personnel

- 2.1 Each Party shall, to the extent it is the relevant Receiving Party, at all times ensure the Processing of the Received Personal Data by natural persons shall be limited to its employees and the employees of its Permitted Recipients (collectively, **personnel**) that need to Process it for the relevant Permitted Purpose in accordance with this Schedule and that all such personnel:

2.1.1 are reliable and have undergone adequate training in the use, care, protection and handling of Received Personal Data as required for compliance with all Data Protection Legislation and this Contract;

2.1.2 are informed of the confidential nature of the Received Personal Data and the relevant party's obligations under this Contract and subject to appropriate obligations of confidentiality;

2.1.3 do not publish, disclose or divulge any of the Received Personal Data to any third party where the party subject to this obligation would not be permitted to do so; and

2.1.4 are subject to (and comply with) a binding written contractual obligation to keep the Received Personal Data confidential (unless disclosure is required under Law).

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Appendix 4
Transparency arrangements

As the Parties are acting as an independent Controllers, the Supplier's processing of Personal Data shall be in accordance with its privacy policy. The Supplier's Privacy Policy can be found at www.vodafone.co.uk/privacy

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Appendix 5
Contact points and reporting

1 Contact Points

1.1 The Contact Point for the Authority is as follows:

dataprotection@justice.gov.uk

1.2 The Contact Point for the Supplier is as follows:

Data.protection@vodafone.com

1.3 The Parties have designated the Contact Points identified above, as the first contact points for third parties in relation to Data Subject Requests and Communications and any other matter relating to the Shared Personal Data. Each Party's respective Contact Point shall have overall internal responsibility within their respective Party for appropriately addressing and responding to Data Subject Requests and Communications within the scope of that Party's obligations.

1.4 Any notice or communication that is required under this Schedule 31 to be sent to a Contact Point shall be sent to the relevant email address of the Contact Point. Such notices and communications shall be deemed delivered in accordance with the same rules specified in Clause 42 (Notices).

2 Reporting

2.1 The Parties each undertake that they shall report to the other Party every 12 months on:

2.1.1 the volume of Data Subject Requests (or purported Data Subject Requests) relating to Shared Personal Data from Data Subjects (or third parties on their behalf); and

2.1.2 any Communications relating to the Shared Personal Data (including any requests for disclosure of the Shared Personal Data which is required or purported to be required by applicable law), that it has received during that period.

3 Governance

3.1 "Data Processing" shall be an agenda item on all relevant Board(s), and the Contact Points shall be responsible for reporting to the Service Board:

3.1.1 the overall effectiveness of the sharing arrangements set out in this Schedule;

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 3.1.2 any Communications or other areas of concern;
 - 3.1.3 whether the objectives as set out in Appendix 2 of this Annex 4 are being met;
 - 3.1.4 whether each Permitted Lawful Basis and Permitted Purpose remain valid and appropriate;
 - 3.1.5 whether the benefits as set out in Appendix 2 of this Annex 4 are being delivered and whether the Shared Personal Data needs to continue to be shared;
 - 3.1.6 whether the privacy notices and arrangements under this Schedule remain appropriate;
 - 3.1.7 the latest quality checks conducted under Appendix 2 of this Annex 4 (or any similar data);
 - 3.1.8 whether the risks of the data sharing have changed; and
 - 3.1.9 whether the technical and organisational measures as set out at Appendix 3 of this Schedule are adequate.
- 3.2 Following each meeting pursuant to this paragraph 3, the Contact Points shall promptly provide a joint report of their findings to the relevant Board.

4 Quality checks

- 4.1 The parties shall each conduct a periodic test of a sample of Shared Personal Data in respect of which it is Disclosing Party to test that it is accurate and up-to-date. Such test shall be conducted at least once in each 12 months of the term of this Contract. The Parties may rely on a test of the same or substantially similar data set which it may have conducted in the previous 12 months, including under other data sharing arrangements with third parties.

5 Review

- 5.1 The Parties shall review periodically the content of this Schedule (the **Review**), which shall include confirmation:
- 5.1.1 that the arrangements reflect current practice and the objectives of the Parties;
 - 5.1.2 that the scope of the Permitted Purpose is still relevant and the scope for which the Shared Personal Data is being used by the Receiving Party has not been expanded without agreement of the Parties;

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 5.1.3 that the benefits to the Data Subjects or society, as stated in Appendix 2 of this Annex 4 are being realised;
 - 5.1.4 whether it would be appropriate to undertake a data protection impact assessment;
 - 5.1.5 whether the arrangements in this Appendix 5 are adequate and working in practice;
 - 5.1.6 that any relevant new guidance issued by any Data Protection Supervisory Authority raised by either party during the Review has been considered as part of the Review;
 - 5.1.7 whether the Shared Personal Data should continue to be shared under this Schedule; and
 - 5.1.8 that the Data Subjects are still the focus of the sharing arrangement and whether their rights are being respected.
- 5.2 The Review shall take place at least every six (6) months during the first two (2) years following its commencement, and at least every twelve (12) months thereafter.

SCHEDULE 31 (PROCESSING PERSONAL DATA)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Appendix 6
Permitted contractors and sub-contractors

Organisation	Permitted Recipient of:	Contact details of organisation's data protection officer or other relevant employee with primary responsibility for the relevant Shared Personal Data within the organisation
[REDACTED]	[REDACTED]	[REDACTED]

SCHEDULE 32 (INTELLECTUAL PROPERTY RIGHTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 32

INTELLECTUAL PROPERTY RIGHTS

SCHEDULE 32 (INTELLECTUAL PROPERTY RIGHTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 32 (*Intellectual Property Rights*)**1 INTELLECTUAL PROPERTY RIGHTS – General Provisions**

1.1 Except as expressly provided for in this Contract or otherwise agreed in writing:

- (a) the Authority and the Service Recipients do not acquire any right, title or interest in or to the Intellectual Property Rights of the Supplier or its licensors, namely:
 - (i) the Supplier Software;
 - (ii) the Third Party Software;
 - (iii) the Third Party IPRs;
 - (iv) the Supplier Background IPRs; and
 - (v) any Know-How, trade secrets or Confidential Information of the Supplier contained in any Specially Written Software or Project Specific IPR; and
- (b) the Supplier does not acquire any right, title or interest in or to the Intellectual Property Rights of the Authority or its licensors and/or the Service Recipients and their licensors, including:
 - (i) the Authority Software;
 - (ii) the Authority Data; and
 - (iii) the Authority Background IPRs; and
- (c) neither Party has the right to use the other Party's (or a Service Recipient's) IPRs, including any use of the other Party's (or a Service Recipient's) names, logos or trademarks .

1.2 Where either Party acquires, by operation of law, ownership of Intellectual Property Rights that is inconsistent with the requirements of this Schedule 32 (*Intellectual Property Rights*), it must assign in writing the Intellectual Property Rights concerned to the other Party on the other Party's request (whenever made).

1.3 If the Supplier becomes aware at any time, including after the Term, that, in respect of any Deliverable, the Authority and/or the Service Recipients have not received the licences to the Supplier Software, the Third Party Software, the Third Party IPRs and the Supplier Background IPRs required by Paragraphs 3 and 6, the Supplier must, within 10 Working Days notify the Authority:

SCHEDULE 32 (INTELLECTUAL PROPERTY RIGHTS)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- (a) the specific Intellectual Property Rights the Authority and/or the Service Recipients have not received licences to; and
 - (b) the Deliverables affected.
- 1.4 Where a patent owned by the Supplier is infringed by the use of the Specially Written Software or Project Specific IPR by the Authority, any Service Recipient or any Replacement Supplier, the Supplier hereby grants to the Authority, the Service Recipients and the Replacement Supplier:
 - (a) a non-exclusive, irrevocable, royalty-free, worldwide patent licence to use the infringing methods, materials or software that expires at the later of
 - (i) the expiry of the Term; or
 - (ii) the expiry of any Termination Assistance Period; and
 - (b) after expiry of the licence granted under Paragraph 1.4(a) and on written request from the Authority, a perpetual, non-exclusive, irrevocable, worldwide patent licence to use the infringing methods, materials or software which must be at a price and on terms no less favourable than those standard commercial terms on which such patent licence is usually made commercially available.
- 1.5 Unless otherwise agreed in writing, the Supplier will record in the table at Annex 1 to this Schedule and keep updated throughout the Term:
 - (a) any Specially Written Software and Project Specific IPR; and
 - (b) where:
 - (i) the Specially Written Software or Project Specific IPR adapts Supplier Software, Third Party Software, Third Party IPRs, or Supplier Background IPRs; or
 - (ii) Supplier Software, Third Party Software, Third Party IPRs, or Supplier Background IPRs is embedded in, or forms an integral part of, the Specially Written Software or Project Specific IPR;

full details of the Supplier Software, Third Party Software, Third Party IPRs, or Supplier Background IPRs.
- 1.6 For the avoidance of doubt:
 - (a) the expiry or termination of this Contract does not of itself terminate the licences granted to the Authority and the Service Recipients under Paragraph 3;
 - (b) the award of this Contract or the ordering of any Deliverables does not constitute an authorisation by the Crown under:

SCHEDULE 32 (INTELLECTUAL PROPERTY RIGHTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (i) Sections 55 and 56 of the Patents Act 1977;
- (ii) section 12 of the Registered Designs Act 1949; or
- (iii) sections 240 to 243 of the Copyright, Designs and Patents Act 1988.

2 OWNERSHIP OF IPR CREATED UNDER THE CONTRACT

2.1 Subject to Paragraph 2.2 the Authority agrees to:

- (a) transfer to the Supplier, or procure the transfer to the Supplier, of all Intellectual Property Rights in Specially Written Software and Project Specific IPRs not already vesting in the Supplier including:
 - (i) the Documentation, Source Code and the Object Code of the Specially Written Software; and
 - (ii) all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software,(together the “**Software Supporting Materials**”); and
- (b) execute or procure the execution of all such assignments required to transfer properly any rights in the Specially Written Software and Project Specific IPRs to the Supplier.

2.2 If within three years of its creation, the Supplier:

- (a) is not commercially exploiting any Specially Written Software, Project Specific IPRs or Software Supporting Materials; or
- (b) where the Supplier is not commercially exploiting that IPR, is not, to the satisfaction of the Authority, using its best endeavours to do so,

then, on written request from the Authority:

- (c) the Supplier must promptly assign to the Authority the Specially Written Software, Project Specific IPRs and Software Supporting Materials, or any specified items of that IPR; and
- (d) the licence to the Authority Software, Authority Data and Authority Background IPRs granted under Paragraph 7.1 (insofar as it relates to the commercial exploitation of the Project Specific IPR, the Specially Written Software or the Software Supporting Materials) terminates either:
 - (i) on the date specified in the notice; or

SCHEDULE 32 (INTELLECTUAL PROPERTY RIGHTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (ii) where no date is specified in the notice, on the date the notice is received by the Supplier.

2.3 Each Party shall bear its own costs of preparing and executing any assignment required by this Paragraph.

3 LICENCE OF SUPPLIER IPR

3.1 The Supplier grants the Authority and the Service Recipients a licence on the terms set out in Paragraph 3.3 in respect of each Deliverable where Specially Written Software, Project Specific IPRs, Software Supporting Materials, Supplier Software or Supplier Background IPRs:

- (a) is embedded in the Deliverable;
- (b) is necessary for the Authority to use the Deliverable;
- (c) in the case of Specially Written Software, Project Specific IPRs, Software Supporting Materials is used to provide the Deliverable;
- (d) in the case of Supplier Software or Supplier Background IPRs has been customised or adapted to create the Deliverable.

3.2 The categories of relevant IPR set out in Paragraph 3.1 are mutually exclusive.

3.3 The licence referred to in Paragraph 3.1 is a non-exclusive, royalty-free, irrevocable, transferable, sub-licensable, worldwide licence that:

- (a) in the case of relevant IPR embedded in a Deliverable, is used to provide the Deliverable, or where the relevant IPR has been customised, configured or adapted to create the Deliverable:
 - (i) is sub-licensable;
 - (ii) has no restriction on the identity of any transferee or sub-licensee;
 - (iii) allows the Authority, the Service Recipients and any transferee or sub-licensee to use, copy and adapt the relevant IPR for any of the purposes set out in Paragraph 3.4;
- (b) in the case of relevant IPR that is necessary for the Authority and the Service Recipients to receive or use the Deliverable:
 - (i) allows the Authority, the Service Recipients and any transferee or sublicensee to use and copy, but not adapt, disassemble or reverse engineer the relevant IPR for any of the purposes set out in Paragraph 3.4;
 - (ii) is transferrable to only:
 - (A) a Crown Body;

SCHEDULE 32 (INTELLECTUAL PROPERTY RIGHTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (B) any body (including any private sector body) that performs or carries out any of the functions or activities that the Authority and/or the Service Recipient had previously performed or carried out; or
 - (C) a person or organisation that is not a direct competitor of the Supplier, where that transferee:
 - enters into a direct arrangement with the Supplier; or
 - enters into a confidentiality arrangement with the Authority in terms equivalent to those set out in set out in Clause 19 (Confidentiality);
- (iii) is sub-licensable to the Replacement Supplier (including where the Replacement Supplier is a competitor of the Supplier) where the Replacement Supplier:
 - (A) enters into a direct arrangement with the Supplier; or
 - (B) enters into a confidentiality arrangement with the Authority in terms equivalent to those set out in set out in Clause 19 (Confidentiality);
- (c) expires at the later of
 - (i) the expiry of the Term; or
 - (ii) the expiry of any Termination Assistance Period; and
- (d) is subject to the restrictions that
 - (i) each transferee or sub-licensee either:
 - (A) enters into a direct arrangement with the Supplier; or
 - (B) enters into a confidentiality arrangement with the Authority in terms equivalent to those set out in set out in Clause 19 (Confidentiality); and
 - (ii) no sub-licence granted to the relevant IPR shall purport to provide the sub-licensee with any wider rights than those granted to the Authority and the Service Recipients under this Paragraph.

3.4 For the purposes of Paragraphs 3.1 and 3.3, the relevant purposes are:

- (a) to allow the Authority, the Service Recipients or any End User to receive and use the Deliverables; and
- (b) for any purpose relating to the exercise of the Authority's, the Service Recipients' (or, if the Authority or Service Recipient is a

SCHEDULE 32 (INTELLECTUAL PROPERTY RIGHTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Public Sector Body, any other Public Sector Body's) business or function.

3.5 Where the legal status of the Authority and/or any Service Recipient changes, such that it ceases to be a Crown Body:

- (a) the licence granted under Paragraph 3.3 is unaffected; and
- (b) any successor body of the Authority and/or Service Recipient that is a Crown Body shall have the benefit of the licence granted under Paragraph 3.3.

3.6 Where the licence granted under Paragraph 3.3 is transferred under Paragraph 3.3(a)(ii) or 3.3(b)(ii) or there is a change in the Authority's and/or any Service Recipient's legal status to which Paragraph 3.5 applies, the transferee or successor body do not acquire any wider rights than those granted to the Authority and/or the Service Recipients under this Paragraph.

4 AUTHORITY APPROVAL FOR SUPPLIER TO EXPLOIT AUTHORITY IPR

4.1 Before using, copying or adapting any:

- (a) Authority Software;
- (b) Authority Data; and
- (c) Authority Background IPRs;

for any purpose other than fulfilling its obligations under this Contract, the Supplier must seek the approval of the Authority in accordance with the provisions of this Paragraph.

4.2 The Authority may terminate any licence it grants under this Paragraph by notice in writing with immediate effect where the Supplier breaches any condition in that licence.

4.3 The Supplier must provide a proposal setting out:

- (a) the purpose for which it proposes to use the IPR;
- (b) the activities the Supplier proposes to undertake with or in respect of the IPR;
- (c) such further information as the Authority may reasonably require to properly consider the proposal.

4.4 The Authority may only refuse the Supplier's proposal where it considers that if the Supplier were to implement the proposal it would harm:

- (a) the Authority's and/or the Service Recipients' reputation; or
- (b) the Authority's and/or the Service Recipients' interests.

4.5 Where the Authority has not:

SCHEDULE 32 (INTELLECTUAL PROPERTY RIGHTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (a) approved or declined the proposal; or
 - (b) required further information,
within 20 Working Days of the later of:
 - (c) the date the proposal was first provided to the Authority; or
 - (d) the date on which further information was provided to the Authority,
- then the proposal is, for the purposes of this Contract, approved.

5 PROVISION OF INFORMATION ON PROJECT SPECIFIC IPR AND SPECIALLY WRITTEN SOFTWARE

5.1 The Authority may, at any time, require the Supplier to provide information on:

- (a) the purposes, other than for the purposes of this Contract, for which the Supplier uses Project Specific IPR and Specially Written Software; and
- (b) the activities the Supplier undertakes, other than under this Contract, with or in respect of the Project Specific IPR and Specially Written Software.

5.2 The Supplier must provide the information required by the Authority:

- (a) within 20 Working Days of the date of the requirement; and
- (b) in the form and with the content specified by the Authority.

6 USE OF THIRD PARTY IPR

6.1 The Supplier must not use any:

- (a) Third Party Non-COTS Software; or
- (b) Third Party Non-COTS Background IPR,

in the provision of the Services (including in any Specially Written Software or in the software element of Project Specific IPRs) unless one of the following conditions is met:

- (c) the owner or an authorised licensor of the relevant IPR has granted the Authority and the Service Recipients a direct licence on the terms equivalent to those set out in Paragraph 3.3 and a copy of the licence has been provided to the Authority; or
- (d) if the Supplier cannot, after commercially reasonable endeavours, meet the condition in Paragraph 6.1(c), all the following conditions are met:
 - (i) the Supplier has notified the Authority in writing giving details of:

SCHEDULE 32 (INTELLECTUAL PROPERTY RIGHTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (A) what licence terms can be obtained from the relevant third party and a copy of the licence has been provided to the Authority; and
 - (B) whether there are providers which the Supplier could seek to use and the licence terms obtainable from those third parties;
- (ii) the Authority approves the licence terms of one of those third parties and such approval is evidenced by the Authority Representative's written approval; and
- (iii) the owner and authorised licensor of the Third Party IPR has granted a direct licence of the Third Party IPR to the Authority and the Service Recipients on those terms; or
- (e) if the Supplier cannot meet the conditions in Paragraphs 6.1(c) and 6.1(d), the Authority has provided written approval to use the relevant IPR without a licence, with reference to the acts authorised and the specific IPR involved.

6.2 The Supplier must not use any:

- (a) Third Party COTS Software; or
- (b) Third Party COTS Background IPR,

in the provision of the Services (including in any Specially Written Software or in the software element of Project Specific IPRs) unless the following conditions are met:

- (c) the Supplier has provided the Authority with the applicable terms for the IPRs (which must be at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available); and
- (d) the Authority approves those licence terms and such approval is evidenced by the Authority Representative's written approval.

7 LICENCES GRANTED BY THE AUTHORITY**7.1 Subject to Paragraph 4, the Authority grants the Supplier a licence to the**

- (a) the Authority Software;
- (b) the Authority Data; and
- (c) the Authority Background IPRs

that:

- (d) is perpetual, non-exclusive, royalty-free and non-transferable;
- (e) is sub-licensable to any Sub-contractor where:

SCHEDULE 32 (INTELLECTUAL PROPERTY RIGHTS)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (i) the Sub-contractor enters into a confidentiality undertaking with the Supplier on the same terms as set out Annex 1 to Schedule 12 (*Software*); and
 - (ii) the sub-licence does not purport to provide the sub-licensee with any wider rights than those granted to the Supplier under this Paragraph;
- (f) allows the Supplier and any sub-licensee to use, copy and adapt any licensed IPRs for the purpose of:
 - (i) fulfilling its obligations under this Contract; or
 - (ii) commercially exploiting the Project Specific IPR, the Specially Written Software or the Software Supporting Materials.

7.2 When the licence granted under Paragraph 7.1:

- (a) terminates in accordance with Paragraph 5; or
- (b) no longer has effect at the end of the Term or the expiry of any Termination Assistance Period (whichever is the later),

the Supplier must, and must ensure that each Sub-contractor granted a sub-licence under Paragraph 7.1(e):

- (c) immediately cease all use of the licensed IPR;
- (d) either:
 - (i) at the discretion of the Authority, return or destroy documents and other tangible materials that contain any of the licensed IPR; or
 - (ii) if the Authority has not made an election within six months of the termination of the licence, destroy the documents and other tangible materials that contain any of the licensed IPR; and
- (e) ensure, so far as reasonably practicable, that any licensed IPR held in electronic, digital or other machine-readable form ceases to be readily accessible from any computer, word processor, voicemail system or any other device of the Supplier.

SCHEDULE 32 (INTELLECTUAL PROPERTY RIGHTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 1: SPECIALLY WRITTEN SOFTWARE AND PROJECT SPECIFIC IPRS

Name of Project Specific IPR	Details

Name of Specially Written Software	Details

Name of adapted or embedded Supplier Software, Third Party Software, Third Party IPRs, or Supplier Background IPRs	Details

SCHEDULE 33 (SERVICE RECIPIENTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SCHEDULE 33
SERVICE RECIPIENTS

SCHEDULE 33 (SERVICE RECIPIENTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Schedule 33 (*Service Recipients*)

1. INTRODUCTION

- 1.1. This Schedule 33 (*Service Recipients*) sets out the basis on which the Supplier shall provide the Services for the benefit not only of the Authority but also for the benefit of the Service Recipients.

2. DEFINITIONS

- 2.1. In this Schedule 33 (*Service Recipients*), the following definitions shall apply:

“Initial Service Recipients” means a body named as such in Annex 1 to this Schedule 33 (*Service Recipients*);

“Potential Service Recipients” means any:

- (a) body named as such in Annex 2 (*Potential Service Recipients*) to this Schedule 33 (*Service Recipients*);
- (b) arms’ length bodies of the Authority;
- (c) body (including any private sector body) created or formed, or brought within the Authority’s responsibility or control, after the date of this Contract; and/or
- (d) body (including any private sector body) which (i) performs any of the functions that previously were performed by the Authority or (ii) to whom the Authority provides services,

in each case added to the list in Annex 1 in accordance with the Change Control Procedure.

“Service Recipients” means:

- (a) the Initial Service Recipients; and
- (b) any Potential Service Recipients;

3. SERVICE RECIPIENTS’ BENEFITS UNDER THE CONTRACT

- 3.1. The Authority has entered into this Contract both for its own benefit and for the benefit of the Service Recipients, provided that nothing in this Contract shall create or be deemed to create a contractual relationship between the Supplier and any Service Recipient.
- 3.2. The Initial Service Recipients who are to benefit under the Contract are identified in Annex 1 to this Schedule 33 (*Service Recipients*). Additional

SCHEDULE 33 (SERVICE RECIPIENTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Service Recipients shall be added to the list in Annex 1 in accordance with the Change Control Procedure.

- 3.3. The Service Recipients shall not be entitled to enforce the relevant provisions of the Contract pursuant to CRTPA.
- 3.4. The Parties to the Contract may in accordance with its provisions vary, terminate or rescind the Contract or any part of it, without the consent of any Service Recipient. No Service Recipient may authorise any Contract Change, Service Request or Project Work Order or any other change to this Contract.
- 3.5. The Authority shall be entitled to enforce any provision of this Contract on behalf of a Service Recipient, but the Supplier shall be liable only to the Authority and shall deal only with the Authority.
- 3.6. Notwithstanding paragraph 3.5 above and subject to paragraph 3.8 below, the Authority may recover all Losses suffered not only by the Authority but also any Losses suffered by any Service Recipient as though it has suffered such Loss itself.
- 3.7. Notwithstanding paragraph 3.5 above and subject to paragraph 3.8 below, the indemnities from the Supplier in the Contract (including those in paragraph 8.9 of Schedule 25 (Exit Management) and Schedule 28 (Staff Transfer)) shall extend not only to Losses suffered or incurred by the Authority but also any Losses suffered or incurred by any Service Recipient.
- 3.8. The Supplier's limits and exclusions of liability in the Contract shall apply as overall limitations on liabilities under this Contract whether relating to a claim by the Authority on behalf of a Service Recipient or to a claim made by the Authority on its own behalf and in no event shall the Authority or any Service Recipient recover twice in respect of the same Loss.
- 3.9. Subject to the Dispute Resolution Procedure, if any breach arises out of any act or omission of a Service Recipient, any claim by the Supplier shall be brought only against the Authority and not against the Service Recipient.
- 3.10. Where compliance with any obligation or responsibility of the Authority is necessary in order to enable the Supplier to supply the benefit of the Services to a Service Recipient, responsibility for compliance shall remain with the Authority but compliance by the Service Recipient shall be deemed to be compliance by the Authority.

SCHEDULE 33 (SERVICE RECIPIENTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 1: INITIAL SERVICE RECIPIENTS

The Services shall be provided for the benefit of the following Initial Service Recipients:

Name of Service Recipient
Academy for Social Justice
Advisory Committees on Justices of the Peace
Assessor of Compensation for Miscarriages of Justice
Civil Justice Council
Civil Procedure Rule Committee
Criminal Injuries Compensation Authority (CICA)
Criminal Procedure Rule Committee
Family Justice Committee
Family Justice Council
Family Procedure Rule Committee
Government Facilities Services Ltd (GFSL)
His Majesty's Courts and Tribunals Service (HMCTS)
His Majesty's Inspectorate of Prisons for England and Wales (HMI Prisons)
His Majesty's Inspectorate of Probation for England and Wales (HMI Probation)
His Majesty's Prison and Probation Service
Independent Advisory Panel on Deaths in Custody
Independent Monitoring Authority (IMA) for the Citizens' Rights Agreements
Independent Monitoring Boards (IMB)
Independent Public Advocate
Insolvency Rules Committee
Judicial Appointments Commission (JAC)
Judicial Appointments and Conduct Ombudsman (JACO)
Judicial Office (JO)
Law Commission
Lay Observers (LO)
Legal Aid Agency (LAA)
National Preventive Mechanism (NPM)
Office of the Public Guardian (OPG)
Official Solicitor and Public Trustee (OPST)
Parole Board
Prison Service Pay Review Body
Prisons and Probation Ombudsman (PPO)
Sentencing Council for England and Wales
Supreme Court
Tribunal Procedure Committee
Victims Commissioner
Wales Office (Office of the Secretary of State for Wales)
Youth Justice Board for England and Wales (YJB)

SCHEDULE 33 (SERVICE RECIPIENTS)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 2: POTENTIAL SERVICE RECIPIENTS

Name of Potential Service Recipient
Children and Family Court Advisory and Support Service (CAFCASS)
Criminal Cases Review Commission (CCRC)
Legal Ombudsman/Office for Legal Complaints
Legal Services Board (LSB)

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

SCHEDULE 34
TRANSITIONAL SERVICES

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

CONTENTS

1 DEFINITIONS AND INTERPRETATION.....5

2 DUE DILIGENCE.....6

3 WARRANTIES.....6

4 TS TERM.....6

5 TRANSITIONAL SERVICES 6

6 IMPLEMENTATION.....8

7 TS PERFORMANCE LEVELS 8

8 SERVICES IMPROVEMENT.....10

9 EQUIPMENT AND MAINTENANCE 10

10 FINANCIAL AND TAXATION MATTERS 10

11 GOVERNANCE 11

12 RECORDS, REPORTS, AUDITS & OPEN BOOK DATA.....11

13 CHANGE.....11

14 SUPPLIER PERSONNEL 12

15 SUPPLY CHAIN RIGHTS AND PROTECTIONS 13

16 INTELLECTUAL PROPERTY RIGHTS 14

17 IPRs INDEMNITY 14

18 AUTHORITY DATA AND SECURITY REQUIREMENTS.....14

19 CONFIDENTIALITY 14

20 TRANSPARENCY AND FREEDOM OF INFORMATION.....15

21 PROTECTION OF PERSONAL DATA 15

22 PUBLICITY AND BRANDING.....15

23 LIMITATIONS ON LIABILITY.....15

24 INSURANCE.....16

25 RECTIFICATION PLAN PROCESS 16

26 DELAY PAYMENTS 16

27 REMEDIAL ADVISER.....17

28 STEP-IN RIGHTS 17

29 AUTHORITY CAUSE.....17

30 FORCE MAJEURE 17

31 TERMINATION RIGHTS.....18

32 CONSEQUENCES OF EXPIRY OR TERMINATION 18

33 COMPLIANCE 19

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

34 ASSIGNMENT AND NOVATION.....20

35 WAIVER AND CUMULATIVE REMEDIES 20

36 RELATIONSHIP OF THE PARTIES 20

37 PREVENTION OF FRAUD AND BRIBERY 20

38 SEVERANCE.....20

39 FURTHER ASSURANCES 20

40 ENTIRE AGREEMENT 20

41 TS THIRD PARTY RIGHTS.....20

42 NOTICES 21

43 DISPUTES 21

44 GOVERNING LAW AND JURISDICTION 21

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEXES

1. TS Definitions
2. Transitional Services Description
3. TS Performance Levels
4. TS Standards
5. TS Security Management
6. Not used
7. Authority TS Responsibilities
8. Supplier TS Solution
9. TS Commercially Sensitive Information
10. Notified TS Key Sub-contractors
11. TS Third Party Contracts
12. TS Software
13. Not used
14. Not Used
15. TS Charges and Invoicing
16. Payments on TS Termination
17. Not used
18. Not used
19. Not used
20. Not used
21. Not used
22. Not used
23. Not used
24. Not used
25. TS Exit Management
26. Not used
27. Not used
28. Not used
29. TS Key Personnel
30. Not used
31. Not used
32. TS Intellectual Property Rights
33. Not used
34. Not used

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Schedule 34 (*Transitional Services*)**1 DEFINITIONS AND INTERPRETATION**

- 1.1 In this Schedule 34, unless otherwise provided or the context otherwise requires;
- (a) capitalised expressions shall have the meanings set out in Annex 1 (*TS Definitions*) to this Schedule 34 or the relevant Annex in which that capitalised expression appears; and
 - (b) references to 'Annex' is a reference to an annex to this Schedule 34 and references to 'Appendix' is a reference to an appendix to an Annex ;and
 - (c) references in any Annex or Appendix to parts, paragraphs, appendices or tables are references to the parts, paragraphs, appendices and tables of the Annex or Appendix in which these references appear.
- 1.2 This Schedule sets out the scope of the Transitional Services and any specific terms and conditions which will apply to the Transitional Services. If there is any conflict between (i) the Paragraphs of this Schedule 34 and (ii) the Annexes and/or the Appendices to this Schedule 34, the conflict shall be resolved in accordance with the following order of precedence:
- (a) the Paragraphs of this Schedule 34;
 - (b) Annexes 2 (*Transitional Services Description*) and 3 (*TS Performance Levels*) and their Appendices;
 - (c) any other Annexes and their Appendices to this Schedule 34 (other than Annex 8 (*Supplier TS Solution*) and its Appendices;
 - (d) Annex 8 (*Supplier TS Solution*) and its Appendices (if any) unless any part of the Supplier TS Solution offers a better commercial position for the Authority (as decided by the Authority, in its absolute discretion), in which case that part of the Supplier TS Solution will take precedence over the documents above.
- 1.3 Except as set out in this Schedule 34 (including the Annexes to Schedule 34) the provisions of this Contract shall apply without amendment in connection with the Transitional Services for the duration of the TS Term.
- 1.4 Where it is stated in this Schedule 34 that a Main Contract Provision will apply in connection with the Transitional Services then, in applying such Main Contract Provision, the provisions of paragraph 1.1 of Annex 1 shall apply.
- 1.5 The terms and conditions set out in this Schedule 34 apply to the Supplier's provision of the Transitional Services only, and shall not affect the operation or application of any Main Contract Provision to the extent it applies to the Supplier's provision of the Services which are not Transitional Services.

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

2 DUE DILIGENCE

2.1 Clauses 2.1 to 2.3 (*Due Diligence*) shall apply.

3 WARRANTIES

3.1 Clauses 3.1 to 3.8 (*Warranties*) shall apply provided that Clause 3.2(h) shall be replaced with the following:

- (h) *all written statements and representations made by the Supplier in the Supplier TS Solution remain true and accurate except to the extent that such statements and representations have been superseded or varied by this Contract or to the extent that the Supplier has otherwise disclosed to the Authority in writing prior to the date of this Contract;*

4 TS TERM

4.1 The Supplier shall, unless terminated at an earlier date by agreement between the Parties, by operation of Law or in accordance with Clause 31 (*Termination Rights*), provide the Transitional Services in accordance with this Schedule 34 until the end of the TS Term.

5 TRANSITIONAL SERVICES**Standard of Transitional Services**

5.1 The Supplier shall provide the Transitional Services from (and including) the Transitional Services Commencement Date for the benefit of the Authority and the Service Recipients.

5.2 The Supplier shall ensure that the Transitional Services:

- (a) comply in all respects with the Transitional Services Description;
- (b) are supplied in accordance with the Supplier TS Solution and the provisions of this Contract; and
- (c) are provided to a standard and level of service which is at least as good as the standard and level of service received by the Authority in respect of the TS Preceding Services in the 12 month period prior to the Effective Date.

5.3 In addition to the obligations set out in Clause 5.3, the Supplier shall perform its obligations in connection with the Transitional Services in accordance with:

- (a) the TS Standards; and
- (b) the TS Baseline Security Requirements.

5.4 In the event that the Supplier becomes aware of any inconsistency between the requirements of Paragraphs 5.3(a) and 5.3(b), the Supplier shall immediately notify the Authority Representative in writing of such inconsistency and the Authority Representative shall, as soon as practicable,

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

notify the Supplier which requirement the Supplier shall comply with.

Supplier covenants

5.5 Clauses 5.5 to 5.8 shall apply:

Continuing obligation to provide the Transitional Services

5.6 The Supplier shall continue to perform all of its obligations under this Contract and shall not suspend the supply of the Transitional Services, notwithstanding:

- (a) any withholding of the TS Service Charges by the Authority pursuant to Paragraph 7.2(d)(ii) (*TS Performance Failures*) of this Schedule 34;
- (b) the existence of an unresolved Dispute; and/or
- (c) any failure by the Authority to pay any TS Charges

Optional Services

5.7 Clauses 5.10 to 5.12 shall not apply.

Power of attorney

5.8 Clause 5.13 shall apply.

Authority TS Responsibilities

5.9 In addition to the responsibilities set out in Schedule 7 (*Authority Responsibilities*), the Authority shall comply with its responsibilities relating to the Transitional Services set out in Annex 7 (*Authority TS Responsibilities*).

Supplier Dependency – TS Gateway

5.10 The Parties agree that the Supplier has the following dependency on the VVI Supplier:

Transitional Service to which the Dependency relates	Who performs the Dependency	Description of Dependency
TS Gateway	VVI Supplier	Dependency on the VVI Supplier to continue providing the VVI Gateway Services, including the Gateway Management Pod, as such are described in the VVI Agreement, until such time as the TS Gateway is no longer required under this Schedule 34, in accordance with the terms and conditions of the VVI Contract.

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

6 IMPLEMENTATION**Quality Plans**

- 6.1 Clauses 6.1 to 6.3 shall apply provided that in Clause 6.3(a), the reference to 'Deliverables' shall include the 'TS Deliverables'.

TS Delays

- 6.2 The Supplier shall ensure that each TS Milestone is Achieved on or before its Milestone Date.
- 6.3 If the Supplier becomes aware that there is, or there is reasonably likely to be a TS Delay, it shall comply with its obligations in Clause 6.6.

Testing and Achievement of TS Milestones

- 6.4 The Parties shall comply with the provisions of Schedule 14 (*Testing Procedures*) in connection with the procedures to determine whether a TS Milestone or Test in respect of a TS Project has been Achieved provided that, in Paragraph 13.2 of Schedule 14, the grant of a Milestone Achievement Certificate in respect of a TS Milestone shall entitle the Supplier to the receipt of a payment in respect of that TS Milestone in accordance with the provisions of Annex 15 (*TS Charges and Invoicing*).

7 TS PERFORMANCE LEVELS

- 7.1 The Supplier shall:
- (a) provide the Transitional Services in such a manner so as to meet or exceed the TS Service Level Target for each TS Service Level and the TS KPI Target for each TS KPI from the Transitional Services Commencement Date; and
 - (b) comply with the provisions of Annex 3 (*TS Performance Levels*) in connection with the monitoring and reporting on its performance against the TS Performance Levels.

TS Performance Failures

- 7.2 If in any Service Period:
- (a) a failure to achieve a TS Service Level Target occurs, TS Service Credits shall be deducted from the TS Service Charges in accordance with Paragraph 6 (*TS Service Credits*) of Annex 15 (*TS Charges and Invoicing*);
 - (b) a TS Service Level Failure occurs that requires the Supplier to put in place a Recovery Plan in accordance with Annex 3 (*TS Performance Levels*), the Supplier shall comply with the requirements in Annex 3 (*TS Performance Levels*) (in addition to TS Service Credits accruing in accordance with Paragraph 7.2(a)(a));

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (c) a TS KPI Failure occurs, the Supplier shall notify the Authority of the action (if any) it will take to rectify the TS KPI Failure and/or to prevent the TS KPI Failure from recurring; and/or
- (d) a Material TS Service Level Failure occurs:
 - (i) the Supplier shall comply with the Rectification Plan Process in accordance with Clause 25; and
 - (ii) the Authority may withhold a proportionate amount of the TS Service Charges in accordance with the process set out in Clause 10.7 (*Set Off and Withholding*) until the relevant Material TS Service Level Failure is rectified to the reasonable satisfaction of the Authority, at which point the Authority shall pay the amount withheld.

7.3 TS Service Credits shall be the Authority's exclusive financial remedy for a TS Service Level Failure except where:

- (a) the Supplier has over the previous 12 month period accrued TS Service Credits in excess of the TS Service Credit Cap;
- (b) the TS Service Level Failure:
 - (i) breaches the relevant TS Service Level Threshold;
 - (ii) has arisen due to the wilful default by the Supplier or any Supplier Personnel; or
 - (iii) results in:
 - (A) the corruption or loss of any Authority Data (in which case the remedies under Clause 18.7 (*Authority Data and Security Requirements*) shall also be available); and/or
 - (B) the Authority being required to make a compensation payment to one or more third parties;
- (c) the Supplier has fraudulently misreported its performance against any TS Service Level; and/or
- (d) the Authority is otherwise entitled to or does terminate the relevant Transitional Services or this Contract pursuant to Clause 31.1(b) (*Termination of by the Authority*).

Critical TS Service Failure

7.4 If a Critical TS Service Failure occurs, the Authority may exercise its rights to terminate this Contract in whole or in part pursuant to Clause 31.1 or 31.2 (*Termination by the Authority*).

Changes to TS Service Levels and TS Service Credits

7.5 Not more than twice in each Contract Year, the Authority may, on giving the

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Supplier at least 2 months' notice, change the TS Service Credit Points that apply in respect of one or more specific TS Service Levels.

- 7.6 The Supplier shall not be entitled to object to any changes made by the Authority under Paragraph 7.5, or increase the TS Service Charges as a result of such changes provided that:
- (a) the total number of TS Performance Levels does not exceed 30;
 - (b) the principal purpose of the change is to reflect changes in the Authority's business requirements and/or priorities or to reflect changing industry standards; and
 - (c) there is no change to the TS Service Credit Cap.

8 SERVICES IMPROVEMENT

- 8.1 Clauses 8.1 to 8.3 shall apply.

9 EQUIPMENT AND MAINTENANCE**Supplier Equipment**

- 9.1 Clauses 9.1 to 9.3 (*Supplier Equipment*) shall apply save that in Clause 9.3, references to the 'Target Performance Levels' shall include the TS Service Level Targets and TS KPI Targets.

Maintenance

- 9.2 Clauses 9.4 to 9.6 shall apply.

Supply of Goods

- 9.3 Clause 9.7 shall apply provided that where the Goods relate to the Transitional Services, the relevant Goods and their prices shall be as set out in the TS Product and Service Catalogue.

Transferring Agreements

- 9.4 Clauses 9.8 and 9.9 shall apply.

10 FINANCIAL AND TAXATION MATTERS**TS Charges And Invoicing**

- 10.1 In consideration of the Supplier carrying out its obligations under this Schedule 34 (*Transitional Services*), including the provision of the Transitional Services, the Authority shall pay the TS Charges to the Supplier in accordance with Annex 15 (*TS Charges and Invoicing*) to this Schedule 34.
- 10.2 Clause 10.2 shall apply. In addition, except as otherwise provided, each Party shall each bear its own costs and expenses incurred in respect of compliance with its obligations under Paragraph 6.5 (*Testing and Achievement of TS Milestones*).

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

10.3 Clause 10.3 shall apply.

VAT

10.4 Clauses 10.4 and 10.5 shall apply.

Set-off and Withholding

10.5 Clause 10.6 shall apply.

10.6 Clause 10.7 shall apply provided that, in Clause 10.7(b), the reference to 'Clause 7.2(d)(ii) (*Performance Failures*)' shall include a reference to Paragraph 7.2(d)(ii) of this Schedule 34 (*TS Performance Failures*).

Benchmarking

10.7 The Authority shall have no right to undertake benchmarking of any or all of the Transitional Services and accordingly Schedule 17 (*Benchmarking*) shall not apply to the Transitional Services.

Financial Distress

10.8 Clause 10.9 shall apply.

Promoting Tax Compliance

10.9 Clause 10.10 shall apply.

11 GOVERNANCE

11.1 Clauses 11.1 to 11.4 shall apply.

12 RECORDS, REPORTS, AUDITS & OPEN BOOK DATA

12.1 Clauses 12.1 and 12.2 shall apply.

13 CHANGE**Change Control Procedure, TS Service Requests and TS Projects**

13.1 Any requirement for a TS Change shall be subject to the Change Control Procedure in Part A of Schedule 22 (*Change Control Procedure, Service Requests and Projects*) provided that:

- (a) in Paragraph 3.2 of Part A of Schedule 22, the cost of any TS Contract Change shall be calculated and charged in accordance with the principles and day rates or day costs (as applicable) set out in Annex 15 (*TS Charges and Invoicing*); and
- (b) in Paragraph 5.5(a) of Part A of Schedule 22, the calculation of costs shall be based on the relevant provisions of Annex 15 (*TS Charges and Invoicing*).

13.2 Any requirement for a TS Service Request or a TS Project shall be subject to the procedures set out in Part B of Schedule 22 (*Change Control Procedure*,

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Service Requests and Projects) provided that:

- (a) in Paragraphs 2.8 , 3.5.3 and 3.7.2 of Part B of Schedule 22, any such payments shall be payable in accordance with Annex 15 (*TS Charges and Invoicing*);
- (b) in Paragraph 4.2.4 of Part B of Schedule 22, the charging basis proposed by the Authority for the intended TS Project shall be by reference to the relevant paragraph of Annex 15 (*TS Charges and Invoicing*);
- (c) in Paragraph 5.2.8 of Part B of Schedule 22, the charges proposed by the Supplier shall be by reference to the relevant prices set out in the relevant paragraph of Annex 15 (*TS Charges and Invoicing*);
- (d) in Paragraph 9.3 of Part B of Schedule 22, a TS Termination Payment shall only be payable by the Authority if applicable in accordance with Annex 16 (*Payments on TS Termination*).

Change in Law

13.3 Clauses 13.2 to 13.4 shall apply.

14 SUPPLIER PERSONNEL

14.1 Clauses 14.1 and 14.2 (*Supplier Personnel*) shall apply provided that:

- (a) the reference in Clause 14.1(b)(ii) to 'Schedule 2 (*Services Description*)' shall include a reference to Annex 2 (*Transitional Services Description*);
- (b) the references in Clause 14.1(b) (ii) and (iii) to 'Schedule 5 (*Security Management*)' shall include a reference to Annex 15 (*TS Security Management*).

TS Key Personnel

14.2 The Supplier shall ensure that the TS Key Personnel fulfil the TS Key Roles at all times during the TS Term. Annex 29 (*TS Key Personnel*) lists the TS Key Roles and names of the persons who the Supplier shall appoint to fill those TS Key Roles at the Effective Date.

14.3 Clauses 14.4 to 14.6 (*Key Personnel*) shall apply.

Employment Indemnity

14.4 Clause 14.7 shall apply.

Income Tax and National Insurance Contributions

14.5 Clause 14.8 shall apply.

Staff Transfer

14.6 Clause 14.9 shall apply.

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

15 SUPPLY CHAIN RIGHTS AND PROTECTIONS**Advertising Sub-contract Opportunities**

15.1 Clauses 15.1 to 15.4 shall apply.

Appointment of Sub-contractors

15.2 Clauses 15.5 to 15.9 shall apply in relation to the appointment of any Sub-contractor in connection with the Transitional Services.

Appointment of TS Key Sub-contractors

15.3 Clauses 15.10 and 15.12 to 15.13 (*Appointment of Key Sub-contractors*) shall apply to the appointment of any TS Key Sub-contractors by the Supplier provided:

- (a) Clause 15.12 shall only apply to TS Key Sub-contracts that relate exclusively to the provision of the Transitional Services to the Authority; and
- (b) the obligation not to materially amend the terms of the TS Key Sub-contract in Clause 15.13 shall only apply to a TS Key Sub-contract that relates exclusively to the provision of the Transitional Services to the Authority.

15.4 The Authority consents to the appointment of the TS Key Sub-contractor(s) listed in Annex 10 (*Notified TS Key Sub-contractors*) in connection with the Transitional Services.

Supply chain protection

15.5 Clause 15.14 shall apply to all Sub-contracts in the Supplier's supply chain made wholly or substantially for the purpose of performing or contributing to the performance of the whole or any part of the Transitional Services.

15.6 Clauses 15.15 to 15.21 shall apply.

Termination of Sub-contracts

15.7 Clause 15.22 (*Termination of Sub-contracts*) shall apply to any Sub-contract relating to the Transitional Services.

Competitive Terms

15.8 Clauses 15.23 and 15.24 shall apply in relation to the supply of any goods, software or services used by the Supplier or the Supplier Personnel in the supply of the Transitional Services.

Retention of Legal Obligations

15.9 Clause 15.25 (*Retention of Legal Obligations*) shall apply in respect of any Sub-contractors engaged (directly or indirectly) by the Supplier in respect of any element of the Transitional Services.

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Exclusion of Sub-contractors

15.10 Clause 15.26 (*Exclusion of Sub-contractors*) shall apply in relation to any Sub-contractors engaged (directly or indirectly) by the Supplier in respect of any element of the Transitional Services.

Reporting SME/VCSE Sub-contracts

15.11 Clauses 15.27 and 15.28 (*Reporting SME/VCSE Sub-contracts*) shall apply.

16 INTELLECTUAL PROPERTY RIGHTS

16.1 The terms and conditions set out in Annex 32 (*TS Intellectual Property Rights*) shall apply.

16.2 The Authority acknowledges that the Supplier shall only be required to provide TS LLDs to the Authority to the extent required under Requirement 8.3.5.6 in Appendix A (*TS Service Management Requirements*) of Annex 2 (*Transitional Services Description*). Where a TS LLD or access to a TS LLD has been provided to the Authority under this Contract, the Authority shall not use such TS LLD for any purpose other than benefiting from the receipt of the Transitional Services, and shall not in any way commercially exploit such TS LLD.

17 IPRs INDEMNITY

17.1 Clauses 17.1 to 17.3 shall apply.

18 AUTHORITY DATA AND SECURITY REQUIREMENTS

18.1 Clauses 18.1 to 18.8 shall apply.

18.2 The Supplier shall comply with the requirements of Annex 5 (*TS Security Management*).

18.3 The Authority shall notify the Supplier of any changes or proposed changes to the TS Baseline Security Requirements.

18.4 If the Supplier believes that a change or proposed change to the TS Baseline Security Requirements will have a material and unavoidable cost implication to the Transitional Services, it may submit a Change Request. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the TS Charges shall then be agreed in accordance with the Change Control Procedure.

18.5 Until and/or unless a change to the TS Charges is agreed by the Authority pursuant to Paragraph 18.4, the Supplier shall continue to perform the Transitional Services in accordance with its existing obligations.

19 CONFIDENTIALITY

19.1 Clauses 19.1 to 19.7 shall apply.

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

20 TRANSPARENCY AND FREEDOM OF INFORMATION

20.1 Clauses 20.1 to 20.8 shall apply.

21 PROTECTION OF PERSONAL DATA21.1 Clauses 21.1 to 21.32 (*Protection of Personal Data*) shall apply to Personal Data in connection with the Transitional Services.**22 PUBLICITY AND BRANDING**

22.1 Clauses 22.1 and 22.2 shall apply.

23 LIMITATIONS ON LIABILITY

23.1 Clauses 23.1 to 23.3 shall apply.

23.2 Clause 23.4 shall apply provided that:

(a) Clause 23.4(c) shall be amended to read:

(c) *the Supplier's aggregate liability in respect of all:*(i) *Service Credits; and*(ii) *Compensation for Unacceptable KPI Failure;**incurred in any Service Period shall be subject to the Service Credit Cap, and the Supplier's aggregate liability in respect of all TS Service Credits incurred in any Service Period shall be subject to the TS Service Credit Cap.*

(b) references to 'Estimated Year 1 Charges' in Clause 23.4(d) shall include all TS Charges payable by the Authority during the first Contract Year.

23.3 Clause 23.5 shall apply.

23.4 Clause 23.6 shall apply provided that Clause 23.6(a) shall be replaced with the following:

(a) *the Authority's and/or a Service Recipient's total aggregate liability in respect of all Losses incurred by the Supplier under or in connection with this Contract as a result of early termination of the Transitional Services by the Authority pursuant to Clause 31.1(a) (Termination of by the Authority), Clause 31.1A (Partial Termination for Convenience) or by the Supplier pursuant to Clause 31.3(a) (Termination by the Supplier) or Clause 34.4 (Assignment and Novation) shall in no event exceed the following amounts:*(i) *in relation to the TS Unrecovered Costs, the amount set out in Paragraph 4 of Annex 16 (Payments on TS Termination); and*(ii) *in relation to the TS Breakage Costs, the amount set out in*

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Paragraph 4 of Annex 16 (Payments on TS Termination).

- (b) references to 'Estimated Year 1 Charges' in Clause 23.6(b)(i) shall include all TS Charges payable by the Authority during the first Contract Year.

Consequential Losses

23.5 Clauses 23.7 and 23.8 shall apply.

Conduct of indemnity claims

23.6 Clause 23.9 shall apply.

Mitigation

23.7 Clause 23.9 shall apply.

24 INSURANCE

24.1 Clause 24.1 shall apply provided that, in addition to its obligations under Clause 24.1, the Supplier shall take out and maintain in force for the duration of the TS Term Professional Indemnity insurance with a limit of indemnity of [REDACTED] in respect of any one claim and in the aggregate per annum.

25 RECTIFICATION PLAN PROCESS

25.1 Clause 25.1 shall apply provided that:

- (a) an additional limb (iii) '*a Material TS Service Level Failure*' shall be added to Clause 25.1(b); and
- (b) the following shall be added as an additional Clause 25.1(d):
- (d) '*a TS Security Management Failure arises*'.

Notification

25.2 Clauses 25.2 and 25.3 shall apply.

Submission of the draft Rectification Plan

25.3 Clauses 25.4 to 25.6 shall apply.

Agreement of the Rectification Plan

25.4 Clauses 25.7 to 25.9 shall apply.

26 DELAY PAYMENTS

26.1 Clauses 26.1 and 26.2 shall apply to TS Projects only if a TS Key Milestone on a TS Project has not been Achieved by the relevant Milestone Date, provided that Clause 26.2(a) shall be replaced with "*the Authority is entitled to*

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

or does terminate the Transitional Services pursuant to Clause 31.1(b) (Termination by the Authority).

27 REMEDIAL ADVISER

27.1 Clauses 27.1 to 27.6 shall apply provided that:

(a) limb (d) of the definition of 'Intervention Trigger Event' in Schedule 1 (*Definitions*) shall be amended to read:

(d) the Supplier accruing (i) Service Credits which meet or exceed 75% of the Service Credit Cap and/or (ii) TS Service Credits which meet or exceed 75% of the TS Service Credit Cap; and/or

(b) limb (e) of the definition of 'Intervention Trigger Event' in Schedule 1 (*Definitions*) shall be amended to read:

(e) the Supplier not Achieving a Key Milestone or a TS Key Milestone within seventy-five (75) days of its relevant Milestone Date;

28 STEP-IN RIGHTS

28.1 Clauses 28.1 to 28.8 shall apply.

29 AUTHORITY CAUSE

29.1 Clauses 29.1 to 29.6 shall apply provided that for the purposes of Clause 29:

(a) a 'Supplier Non-Performance' shall include a reference to a failure to provide the Transitional Services in accordance with the TS Service Level Targets and/or TS KPI Targets; and

(b) Clause 29.1(iv)(B) shall include a reference to the Authority's right to withhold any of the TS Service Charges pursuant to Paragraph 7.2(d)(ii) (*TS Performance Failures*) of Schedule 34.

30 FORCE MAJEURE

30.1 Clauses 30.1 to 30.8 shall apply provided that Clause 30.6(b)(C) shall be amended to read:

(C) to receive Service Credits or TS Service Credits, to withhold any of the Service Charges pursuant to Clause 7.2(d)(ii) (Performance Failures) or any of the TS Service Charges pursuant to Paragraph 7.2(d)(ii) (TS Performance Failures) of Schedule 34 and retain any of the Service Charges as compensation pursuant to Clause 7.4(a) (Unacceptable KPI Failure) to the extent that a Performance Failure or a TS Service Level Failure (as appropriate) has been caused by the Force Majeure Event;

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

31 TERMINATION RIGHTS**Termination by the Authority**

- 31.1 Clause 31.1 shall apply provided that the reference in limb (a) of the definition of 'Supplier Termination Event' in Schedule 1 (*Definitions*) to a Critical Performance Failure shall include a Critical TS Service Failure.

Partial Termination for Convenience

- 31.2 Clauses 31.1A and 31.2 shall apply.

Termination by the Supplier

- 31.3 Clause 31.3 shall apply.

Partial Termination

- 31.4 Clauses 31.4 and 31.5 shall apply.

32 CONSEQUENCES OF EXPIRY OR TERMINATION**General Provisions on Expiry or Termination**

- 32.1 The provisions of:

- (a) Clauses 5.8 (*Specially Written Software warranty*), 9.7(f) (*Indemnity against the recall of goods*), 10.4 and 10.5 (*VAT*), 10.6 and 10.7 (*Set-off and Withholding*), 12 (*Records, Reports, Audits and Open Book Data*), 14.7 (*Employment Indemnity*), 14.8 (*Income Tax and National Insurance Contributions*), 17.1 (*IPRs Indemnity*), 19 (*Confidentiality*), 20 (*Transparency and Freedom of Information*), 21 (*Protection of Personal Data*), 38 (*Severance*), 39.1 40 (*Entire Agreement*), 42.1 43 (*Disputes*) and 43.1 44 (*Governing Law and Jurisdiction*);
- (b) Paragraphs 16 (*Intellectual Property Rights*), 23 (*Limitations on Liability*), 32 (*Consequences of Expiry or Termination*), 41 (*Third Party Rights*) of this Schedule 34; and
- (c) Annexes 1 (*TS Definitions*), 15 (*TS Charges and Invoicing*), 16 (*Payments on TS Termination*), 25 (*TS Exit Management*) and 32 (*TS Intellectual Property Rights*);

shall survive the termination or expiry of this Contract and/or the Transitional Services.

- 32.2 Clause 32.2 shall apply.

Exit Management

- 32.3 The Parties shall comply with the provisions of Annex 25 (*TS Exit Management*) and any current TS Exit Plan in connection with the expiry of

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

the Transitional Services or the orderly transition of the Transitional Services to the Authority or a Replacement Supplier.

Payments by the Authority

32.4 If this Contract or the Transitional Services are terminated by the Authority pursuant to Clause 31.1(a) (*Termination by the Authority*) or by the Supplier pursuant to Clause 31.3(a) (*Termination by the Supplier*) or Clause 34.4 (*Assignment and Novation*), the Authority shall pay the Supplier the TS Termination Payment (calculated in accordance with Annex 16 (*Payments on TS Termination*)) (which shall be the Supplier's sole remedy for the termination of the Transitional Services).

32.5 Clause 32.5 shall apply provided that Clause 32.5(a) shall be amended to read:

(a) *payments in respect of any TS Assets or apportionments in accordance with Annex 25 (TS Exit Management) and/or payments in respect of any Assets or apportionments in accordance with Schedule 25 (Exit Management).*

32.6 Clause 32.6 shall apply.

Payments by the Supplier

32.7 Clauses 32.7 to 32.12 shall apply.

33 COMPLIANCE**Health and Safety**

33.1 Clauses 33.1 and 33.2 shall apply.

Employment Law

33.2 Clause 33.3 shall apply.

Equality and Diversity

33.3 Clause 33.4 shall apply.

Official Secrets Act and Finance Act

33.4 Clause 33.5 shall apply.

Conflicts of Interest

33.5 Clauses 33.6 and 33.7 shall apply.

Modern Slavery

33.6 Clauses 33.8 to 33.12 shall apply.

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

Whistleblowing

33.7 Clause 33.13 shall apply.

34 ASSIGNMENT AND NOVATION

34.1 Clauses 34.1 to 34.4 shall apply.

35 WAIVER AND CUMULATIVE REMEDIES

35.1 Clauses 35.1 and 35.2 shall apply.

36 RELATIONSHIP OF THE PARTIES

36.1 Clause 36.1 shall apply.

37 PREVENTION OF FRAUD AND BRIBERY

37.1 Clauses 37.1 to 37.7 shall apply.

38 SEVERANCE

38.1 Clause 38.1 shall apply.

39 FURTHER ASSURANCES

39.1 Clause 39.1 shall apply.

40 ENTIRE AGREEMENT

40.1 Clauses 40.1 to 40.3 shall apply.

41 TS THIRD PARTY RIGHTS

41.1 The provisions of Paragraphs 17.1 (*IPRs Indemnity*) and the provisions of Paragraph 6.11 of Part A of Annex 25 (*TS Exit Management*) (together "**TS Third Party Provisions**") confer benefits on persons named or identified in such provisions other than the Parties (each such person a "**TS Third Party Beneficiary**") and are intended to be enforceable by TS Third Parties Beneficiaries by virtue of the CRTPA.

41.2 Subject to Paragraph 41.1, a person who is not a Party to this Contract has no right under the CRTPA to enforce any term of this Schedule 34 but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.

41.3 No TS Third Party Beneficiary may enforce, or take any step to enforce, any TS Third Party Provision without the prior written consent of the Authority, which may, if given, be given on and subject to such terms as the Authority may determine.

41.4 Any amendments or modifications to this Schedule 34 may be made, and any rights created under Paragraph 41.1 may be altered or extinguished, by the Parties without the consent of any TS Third Party Beneficiary.

SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

42 NOTICES

42.1 Clauses 42.1 to 42.6 shall apply.

43 DISPUTES

43.1 Clauses 43.1 and 43.2 shall apply.

44 GOVERNING LAW AND JURISDICTION

44.1 Clauses 44.1 and 44.2 shall apply.

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 1

TS DEFINITIONS

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Annex 1 (*TS Definitions*)

1 DEFINITIONS

1.1 In this Schedule 34, unless the context otherwise requires;

1.1.1 capitalised expressions that are defined in Part A of this Annex (or another Annex to this Schedule 34) shall have the meaning set out in Part A of this Annex 1 (or the relevant Annex in which that capitalised expression appears);

1.1.2 where it is stated that a Main Contract Provision will apply in connection with the Transitional Services then, in applying such Main Contract Provision, capitalised expressions used in the relevant Main Contract Provision which are listed in Column 1 in the table in Part B of this Annex 1 shall be read as meaning or including (as appropriate) the relevant TS Definition listed in Column 2 in the table in Part B of this Annex; and

1.1.3 capitalised expressions that are not defined in Part A or Part B of this Annex, or elsewhere in this Schedule 34, but are defined in Schedule 1 (*Definitions*) (or any other Schedule of this Contract), shall have the meanings given in Schedule 1 (or the relevant Schedule).

1.2 If a capitalised expression does not have an interpretation in this Annex 1, Schedule 1 (or any other Schedule) of this Contract, or any other Annex, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.

1.3 In this Schedule 34 (Transitional Services), unless the context otherwise requires:

1.3.1 the singular includes the plural and vice versa;

1.3.2 reference to a gender includes the other gender and the neuter;

1.3.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Crown Body;

1.3.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;

1.3.5 the words **including**, **other**, **in particular**, **for example** and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words **without limitation**;

1.3.6 references to **writing** include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 1.3.7 references to **representations** shall be construed as references to present facts, to **warranties** as references to present and future facts and to **undertakings** as references to obligations under the Contract;
 - 1.3.8 references to **Schedules** are, unless otherwise provided, references to the Schedules of this Contract and references in any Annex to parts, parts, paragraphs, appendices and tables are, unless otherwise provided, references to the parts, paragraphs, appendices and tables of the Schedule in which these references appear;
 - 1.3.9 references to **Annexes** and **Appendixes** are, unless otherwise provided, references to the Annexes and Appendixes of this Schedule 34 and references in any Annex to parts, paragraphs, appendices and tables are, unless otherwise provided, references to the parts, paragraphs, appendices and tables of the Annex in which these references appear;
 - 1.3.10 references to **Clauses** are, unless otherwise provided, references to the clauses of the Core Terms;
 - 1.3.11 references to **Paragraphs** are, unless otherwise provided, references to the paragraph of this Schedule 34 or of the appropriate Annex unless otherwise provided;
 - 1.3.12 references to a series of Clauses or Paragraphs shall be inclusive of the clause numbers specified;
 - 1.3.13 the headings in Schedule 34 are for ease of reference only and shall not affect the interpretation or construction of Schedule 34;
 - 1.3.14 where the Authority is a Crown Body, it shall be treated as contracting with the Crown as a whole; and
 - 1.3.15 the expressions listed in ITIL shall have the meanings given to them in ITIL and this shall also apply to ITIL expressions that may be used in this Contract with a capital first letter, but which are listed in ITIL with a lower-case first letter.
- 1.4 Any reference in this Schedule 34 which immediately before IP Completion Day (or such later date when relevant EU law ceases to have effect pursuant to Section 1A of the European Union (Withdrawal) Act 2018) is a reference to (as it has effect from time to time):
- (a) any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement (**EU References**) which is to form part of domestic law by application of Section 3 of the European Union (Withdrawal) Act 2018 shall be read on and after IP Completion Day as a reference to the EU References as they form part of domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 as modified by domestic law from time to time; and

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) any EU institution or EU authority or other such EU body shall be read on and after IP Completion Day as a reference to the UK institution, authority or body to which its functions were transferred.
- 1.5 Where a standard, policy or document is referred to in this Schedule 34 by reference to a hyperlink, then if the hyperlink is changed or no longer provides access to the relevant standard, policy or document, the Supplier shall notify the Authority and the Parties shall update this Schedule 34 with a reference to the replacement hyperlink.
- 1.6 If there is any conflict between the meaning given to an expression in ITIL and the meaning given to the expression in this Annex 1 (*TS Definitions*), then the meaning given to that expression in this Annex 1 (*TS Definitions*) shall apply. Paragraph 1.3.15 shall apply to ITIL expressions that may be used in this Schedule 34 with a capital first letter, but which are listed in ITIL with a lower-case first letter.

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Part A: TS Definitions

This Part A sets out the definitions which apply specifically in connection with the Transitional Services and are used in this Schedule 34 and its Annexes.

Authority TS Assets

the Authority TS Materials, the Authority infrastructure and any other data, software, assets, equipment or other property owned by and/or licensed or leased to the Authority and which is or may be used in connection with the provision or receipt of the Transitional Services;

Authority TS Cause

any material failure by the Authority to perform any of the Authority's obligations as set out in Annex 7 (*Authority TS Responsibilities*), in each case, except to the extent that such breach is:

- (a) the result of any act or omission by the Authority (as applicable) to which the Supplier has given its prior written consent; or
- (b) caused by the Supplier, any Sub-contractor or any Supplier Personnel;

Authority TS Materials

the Authority Data together with any materials, documentation, information, programs and codes supplied by the Authority and/or a Service Recipient to the Supplier, the IPRs in which:

- (a) are owned or used by or on behalf of the Authority and/or a Service Recipient; and
- (b) are or may be used in connection with the provision or receipt of the Transitional Services,

but excluding any TS Project Specific IPRs, TS Specially Written Software, TS Supplier Software, TS Third Party Software and TS Documentation relating to TS Supplier Software or TS Third Party Software;

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Authority TS Requirements	the requirements of the Authority set out in Annex 2 (<i>Transitional Services Description</i>), Annex 3 (<i>TS Performance Levels</i>), Annex 4 (<i>TS Standards</i>), Annex 5 (<i>TS Security Management</i>), Annex 13 (<i>TS Implementation</i>) and Annex 25 (<i>TS Exit Management</i>);
Authority TS Responsibilities	the responsibilities of the Authority in connection with the Transitional Services specified in: (a) Paragraphs 1 and 2 of Schedule 7 (Authority Responsibilities); and (b) Annex 7 (Authority TS Responsibilities);
Certificate of TS Costs	has the meaning given in Paragraph 7.1 of Annex 15 (<i>TS Charges and Invoicing</i>);
Critical TS Service Failure	a failure identified as a critical service failure in Annex 3 (<i>TS Service Levels</i>);
[REDACTED]	[REDACTED]
Exception Report	has the meaning given in Annex 3 (<i>TS Performance Levels</i>);
GovWiFi	means a Wi-Fi authentication service allowing staff and visitors to use a single username and password to connect to guest Wi-Fi across the public sector;
Incident	a Service Incident and/or a Security Incident;
Incident Management System	has the meaning given in Annex 3 (<i>TS Performance Levels</i>);
Incident Resolution Priority	has the meaning given in Annex 3 (<i>TS Performance Levels</i>);
Incident Resolution Time	has the meaning given in Annex 3 (<i>TS Performance Levels</i>);

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Indexation and Index	the adjustment of an amount or sum in accordance with Paragraph 2.8 of Annex 15 (<i>TS Charges and Invoicing</i>);
Main Contract Provision	a provision of the Core Terms or a Schedule (other than this Schedule 34);
Material TS Service Level Failure	has the meaning given in Annex 3 (<i>TS Performance Levels</i>);
Maximum TS Service Credit Points to Reach Cap	means the value identified in Paragraph 6.2 of Annex 15 (<i>TS Charges and Invoicing</i>);
Net Book Value	the net book value of the relevant TS Asset(s) calculated in accordance with the depreciation policy of the Supplier set out in the letter in the agreed form from the Supplier to the Authority of the same date as the Effective Date;
New TS Assets	has the meaning given in Paragraph 5.2 of Annex 16 (<i>Payments on TS Termination</i>);
Notified TS Key Sub-contractor	a TS Key Sub-contractor listed in Annex 10 (Notified TS Key Sub-contractors);
Person Day Resources	the Supplier Personnel that perform work/Services under a Project Work Order where such work is to be charged using the TS Time and Materials Charges mechanism;
Person Day	7.5 Person Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day;
Person Hour	the hours spent by the Supplier Personnel properly working on the Transitional Services including time spent travelling (other than to and from the Supplier's offices, or to and from the premises at which the services are to be principally performed) but excluding lunch breaks;
Recovery Plan	has the meaning given in Annex 3 (<i>TS Performance Levels</i>);

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Service Operations Manual	shall mean the TS Service Operations Manual;
Supplier TS Equipment	the hardware, computer and telecoms devices and equipment used by the Supplier or its Sub-contractors (but not hired, leased or loaned from the Authority) for the provision of the Transitional Services;
Supplier TS Solution	the Supplier's solution for the Transitional Services set out in Annex 8 (<i>Supplier TS Solution</i>) including any Appendices to that Annex;
Supplier TS System	the information and communications technology system used by the Supplier in implementing and performing the Transitional Services including the TS Software, the Supplier TS Equipment, configuration, monitoring and management utilities, calibration and testing tools and related cabling (but excluding the Authority System);
Transitional Services	any and all of the services to be provided by the Supplier under this Schedule 34, including those set out in Annex 2 (<i>Transitional Services Description</i>);
Transitional Services Description	the services description set out in Annex 2 (<i>Transitional Services Description</i>);
TS Assets	all assets and rights used by the Supplier to provide the Transitional Services in accordance with this Schedule 34 but excluding the Authority TS Assets;
TS ATP Milestone	the TS Milestone linked to Authority to Proceed for the relevant Transitional Services set out in a TS Project Plan;
TS Background IPRs	(a) Intellectual Property Rights owned by the Supplier before the Effective Date, for example those subsisting in the Supplier's standard development tools, program components or standard code used in computer

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

programming or in physical or electronic media containing the Supplier's Know-How or generic business methodologies; and/or

- (b) Intellectual Property Rights acquired or created by the Supplier independently of, or for purposes that are not exclusively for the performance of, the Transitional Services,

which in each case is or will be used before or during the TS Term for designing, testing implementing or providing the Transitional Services but excluding Intellectual Property Rights owned by the Supplier subsisting in the Supplier Software;

TS Baseline Security Requirements

has the meaning given to that term in Part A of Annex 5 (*TS Security Management*);

TS Breakage Costs

an amount determined in accordance with Paragraph 4.1(e) of Annex 16 (*TS Payments on Termination*);

TS Capacity Plan

means the plan referred to in in Paragraph 4.3.3. of Appendix A (*TS Service Management Requirements*) to Annex 2 (*Transitional Services Description*) which ensures the Supplier delivers sufficient capacity to cope with:

- (a) all known contingencies for the Transitional Services;
- (b) planned expansion or contraction of the Transitional Services; and
- (c) the Transitional Services to be delivered to the Authority by the Supplier and any Other Supplier that has a dependency on the Transitional Services

TS Catalogue Item

means a product or service described within the TS Product and Service Catalogue;

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

TS Catalogue Owner	means the Authority's owner of the TS Product and Service Catalogue as notified to the Supplier by the Authority;
TS Change	any change to this Schedule 34;
TS Charges	the charges for the provision of the Transitional Services set out in or otherwise calculated in accordance with Annex 15 (<i>TS Charges and Invoicing</i>) including any TS Milestone Payment or TS Service Charge;
TS Commercially Sensitive Information	has the meaning given in Paragraph 1 of Annex 9 (<i>TS Commercially Sensitive Information</i>);
TS Configuration Item	means any Transitional Services component, infrastructure element, or other item that needs to be managed in order to ensure the successful delivery of the Transitional Services;
TS Continual Service Improvement	means the process that ensures the Transitional Services remain aligned with the changing needs of the Authority's business by identifying and implementing improvements to the Transitional Services;
TS Contract Change	any change to this Schedule 34 other than a TS Operational Change;
TS Core Information Management System or TS CIMS	has the meaning given in Paragraph 1 of Part A of Annex 5 (<i>TS Security Management</i>);
TS COTS Background IPRs	any embodiments of TS Background IPRs that: (a) the Supplier makes generally available commercially prior to the date of this Contract (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price; and

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	(b) has a Non-trivial Customer Base;
TS COTS Software	TS Supplier Software (including open source software) that: (a) the Supplier makes generally available commercially prior to the date of this Contract (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price; and (b) has a Non-trivial Customer Base;
TS CPP Milestone	a contract performance point as set out in a TS Project Plan, being the TS Milestone at which the Supplier has demonstrated that the Supplier TS Solution or relevant Transitional Service is working satisfactorily in its operating environment in accordance with Schedule 14 (<i>Testing Procedures</i>);
TS Deductions	all TS Service Credits, TS Delay Payments or any other deduction which is paid or payable to the Authority under this Schedule 34;
TS Defect	(a) any error, damage or defect in the manufacturing of a TS Deliverable; or (b) any error or failure of code within the TS Software which causes a TS Deliverable to malfunction or to produce unintelligible or incorrect results; or (c) any failure of any TS Deliverable to provide the performance, features and functionality specified in the Authority TS Requirements or the TS Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant TS Deliverable from meeting its associated Test Success Criteria; or

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (d) any failure of any TS Deliverable to operate in conjunction with or interface with any other TS Deliverable in order to provide the performance, features and functionality specified in the Authority TS Requirements or the TS Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant TS Deliverable from meeting its associated TS Test Success Criteria;

TS Delay Deduction Period the period set out in the relevant Project Work Order for a TS Project commencing on the relevant Milestone Date;

TS Delay Payments the amounts payable by the Supplier to the Authority in respect of a TS Delay;

- TS Delay**
- (a) a delay in the Achievement of a TS Milestone by its Milestone Date; or
 - (b) a delay in the design, development, testing or implementation of a TS Deliverable by the relevant date set out in the relevant TS Project Plan;

TS Deliverable an item, feature or software delivered or to be delivered by the Supplier at or before a Milestone Date or at any other stage during the performance of a TS Project which may be either a TS Documentary Deliverable or a TS Non-Documentary Deliverable;

TS Documentary Deliverable a deliverable in connection with the Transitional Services that takes the form of TS Documentation;

TS Documentation descriptions of the Transitional Services and TS Performance Levels, details of the Supplier TS System (including (i) vendors and versions for off-the-shelf components and (ii) source code and build information for proprietary software components), relevant design and development information,

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

technical specifications of all functionality including those not included in standard manuals (such as those that modify system performance and access levels), configuration details, test scripts, user manuals, operating manuals, process definitions and procedures, and all such other documentation as:

- (a) is required to be supplied by the Supplier to the Authority under this Contract (other than through the operation of this limb (a) of this definition); and/or
- (b) not used
- (c) is required by the Supplier in order to provide the Transitional Services; and/or
- (d) has been or shall be generated for the purpose of providing the Transitional Services,

provided that documentation will not include: (A) documentation which is created for the Supplier's own internal purposes; (B) documentation which is not created in the performance of the Transitional Services; or (C) LLDs (without prejudice to the Supplier's obligations to provide LLDs to the Authority under Clause 16.2, Annex 2 (*TS Services Description*) or Schedule 24 (*Reports and Records*);

TS Financial Model

the financial model agreed between the Parties (as amended and updated in accordance with Schedule 19 (*Financial Reports and Audit Rights*) in relation to the Transitional Services;

TS Gateway

shall have the meaning given in Paragraph 2.4 of Appendix B (*TS Technical Requirements*) to Annex 2 (*Transitional Services Specification*);

TS Hardened Builds

means the configuration of firewalls, switches, servers, routers to remove

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	unsecure protocols, lock down unsecure features and functionality offered in the base manufacturer software/firmware as created by the Supplier independently of this Contract that forms part of the TS Non-COTS Background IPRs but excluding any Authority specific configuration (e.g. firewall rule-bases) which forms part of the TS Project Specific IPRs;
“TS HLD”	means the high-level design describing the overall architecture and description of the Transitional Services and Supplier TS Solution;
TS Incident	a TS Service Incident or a Security Incident;
TS IPRs Claim	any claim against any Indemnified Person of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any TS Relevant IPRs save for any such claim to the extent that it is caused by (a) any use by or on behalf of that Indemnified Person of any TS Relevant IPRs in combination with any item not supplied or recommended by the Supplier pursuant to this Schedule 34 or for a purpose not reasonably to be inferred from the Transitional Services Description or the provisions of this Contract, or (b) the use of the TS Software or Authority Software by or on behalf of the Supplier;
TS IT Environment	the Authority System and the Supplier TS System;
TS ITSCM Plan	shall have the meaning given in Paragraph 4.4.4.4 of Appendix A (<i>TS Service Management Requirements</i>) to Annex 2 (<i>Transitional Services Description</i>);
TS Key Milestone	the TS Milestones identified in a Change Authorisation Note as key milestones for a TS Project and in respect of which TS Delay Payments may be payable if the Supplier

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	fails to Achieve the Milestone Date in respect of such TS Milestone;
TS Key Performance Indicator (or TS KPI)	has the meaning given in Annex 3 (<i>TS Performance Levels</i>);
TS Key Personnel	those persons appointed by the Supplier to fulfil the TS Key Roles, being the persons listed in Annex 29 (<i>TS Key Personnel</i>) against each TS Key Role as at the Effective Date or as amended from time to time in accordance with Clauses 14.5 and 14.6 (Key Personnel);
TS Key Roles	a role described as a key role in Annex 29 (<i>TS Key Personnel</i>) and any additional roles added from time to time in accordance with Clause 14.4 (Key Personnel);
TS Key Sub-contract	each Sub-contract with a TS Key Sub-contractor;
TS Key Sub-contractor	any Sub-contractor: (a) which, in the opinion of the Authority, performs (or would perform if appointed) a critical role in the provision of all or any part of the Transitional Services; and/or (b) with a Sub-contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the aggregate TS Charges forecast to be payable under this Schedule 34 as set out in the TS Financial Model;
TS KPI Failure	a failure to meet the KPI Target in respect of a KPI as set out in Annex 3 (<i>TS Performance Levels</i>);
TS KPI Target	has the meaning given in Annex 3 (<i>TS Performance Levels</i>);
TS Licensed Software	all and any software licensed by or through the Supplier, its Sub-contractors or any third

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	party to the Authority for the purposes of or pursuant to this Schedule 34, including any TS Supplier Software, TS Third Party Software and/or any TS Specially Written Software;
TS LLDs	means low level design documents including detailed functional interpretation of the TS HLD;
TS Management Information	the management information specified in Annex 3 (<i>TS Performance Levels</i>) and Annex 15 (<i>TS Charges and Invoicing</i>) to be provided by the Supplier to the Authority;
TS Milestone	an event or task described in a TS Project Plan which, if applicable, shall be completed by the relevant Milestone Date;
TS Milestone Adjustment Payment Notice	a Milestone Adjustment Payment Notice in respect of a TS Project issued in accordance with Clause 32.7 (<i>Payments by the Supplier</i>);
TS Milestone Payment	a payment identified in Annex 15 (<i>TS Charges and Invoicing</i>) to be made following the issue of a Milestone Achievement Certificate;
TS New Releases	an item produced primarily to extend, alter or improve the TS Software and/or any TS Deliverable by providing additional functionality or performance enhancement (whether or not defects in the TS Software and/or TS Deliverable are also corrected) while still retaining the original designated purpose of that item;
TS Non-COTS Background IPRs	any embodiments of TS Background IPRs that have been delivered by the Supplier to the Authority and that are not TS COTS Background IPRs;
TS Non-COTS Software	TS Supplier Software that is not TS COTS Software;

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

TS Non-Documentary Deliverables	any TS Deliverables excluding TS Documentary Deliverables;
TS Operational Change	any change in the Supplier's operational procedures which in all respects, when implemented: (a) will not affect the TS Charges and will not result in any other costs to the Authority; (b) may change the way in which the Transitional Services are delivered but will not adversely affect the output of the Transitional Services or increase the risks in performing or receiving the Transitional Services; (c) will not adversely affect the interfaces or interoperability of the Transitional Services with any of the Authority's IT infrastructure; and (d) will not require a change to this Schedule 34;
TS Performance Levels	has the meaning given in Annex 3 (<i>TS Performance Levels</i>);
TS Preceding Services	services similar to the Transitional Services which the Authority was receiving immediately prior to the Effective Date;
TS Problem	the cause or one or more TS Incidents'
TS Product and Service Catalogue	the product and services catalogue that details the TS Catalogue Items that can be ordered by the Authority in accordance with the Service Request procedure in Part B of Schedule 22 (<i>Change Control Procedure, Service Requests and Projects</i>);
TS Project	the programme of work undertaken in connection with the Transitional Services pursuant to a Project Work Order agreed by the Parties in accordance with the procedures set out in Schedule 22 (<i>Change</i>

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	<i>Control Procedure, Service Requests and Projects);</i>
TS Project Daily Rate	the day rates applicable to TS Rate Card Services as set out in Appendix D to Annex 15 (<i>TS Charges and Invoicing</i>);
TS Project Specific IPRs	(a) Intellectual Property Rights in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of the Transitional Services and updates and amendments of these items including (but not limited to) database schema; and/or (b) Intellectual Property Rights arising as a result of the performance of the Supplier's obligations under this Schedule 34, but shall not include the TS Background IPRs or the TS Specially Written Software and provided that limb (b) above will not include Intellectual Property Rights subsisting in items or materials created for the Supplier's own internal purposes only;
TS Rate Card Services	has the meaning given in Paragraph 4.1 of Annex 15 (<i>TS Charges and Invoicing</i>);
TS Register	has the meaning given in Paragraph 2.2.1 of Annex 25 (<i>TS Exit Management</i>);
TS Relevant IPRs	IPRs used to provide the Transitional Services or as otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Authority or a third party in the fulfilment of the Supplier's obligations under this Schedule 34 including IPRs in the TS Specially Written Software, the TS Non-COTS Software, the TS Non-COTS Background IPRs, the TS Third Party Non-COTS Software and the TS Third Party Non-COTS IPRs but excluding any IPRs in the Authority Software, the Authority Background

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

IPRs, the TS COTS Software, the TS COTS Background IPRs, the TS Third Party COTS Software and/or the TS Third Party COTS IPRs;

TS Security Audit

means such regular audits as the Supplier is required to perform for the Authority in order to demonstrate the Transitional Services are aligned with the Authority's security policies, processes, procedures, standards and guidelines;

TS Security Management Failure

the occurrence of any of the events in Paragraphs 6.15.2, 8.12, 9.8 and 11.4 of Annex 5 (*TS Security Management*) requiring the Supplier to prepare a Rectification Plan;

TS Security Management Plan

has the meaning given in Annex 5 (*TS Security Management*);

TS Service Assets

all assets and rights used by the Supplier to provide the Transitional Services in accordance with this Schedule 34 including TS Assets and Authority TS Assets;

TS Service Availability

has the meaning given in Annex 3 (*TS Performance Levels*);

TS Service Change

means any change to the Supplier TS System as described in the Change and Evaluation Management Process;

TS Service Charges

the periodic payments made in accordance with Annex 15 (*TS Charges and Invoicing*) in respect of the supply of the Transitional Services, as set out in Paragraph 3 of Annex 15 (*TS Charges and Invoicing*);

TS Service Credit Cap

has the meaning given in Paragraph 6.3 of Annex 15 (*TS Charges and Invoicing*);

TS Service Credit Point

has the meaning given in Annex 3 (*TS Performance Levels*);

TS Service Credit Regime

has the meaning given in Annex 3 (*TS Performance Levels*);

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

TS Service Credits	credits payable by the Supplier due to the occurrence of 1 or more TS Service Level Failures, calculated in accordance with Paragraph 3 of Annex 15 (<i>TS Charges and Invoicing</i>);
TS Service Level	has the meaning given in Annex 3 (<i>TS Performance Levels</i>);
TS Service Level Failure	has the meaning given in Annex 3 (<i>TS Performance Levels</i>);
TS Service Level Target	has the meaning given in Annex 3 (<i>TS Performance Levels</i>);
TS Service Level Threshold	has the meaning given in Annex 3 (<i>TS Performance Levels</i>);
TS Service Line	has the meaning given in Annex 3 (<i>TS Performance Levels</i>);
TS Service Management Requirements	means the requirements as described in Appendix A – TS Service Management Requirements to Annex 2 (<i>Transitional Services Description</i>);
TS Service Operations Manual	the Supplier's service operations manual for the provision of the Transitional Services as set out in Appendix 2 to Annex 4 (<i>TS Standards</i>);
TS Service Request	a TS Service Request enables the Authority to order TS Catalogue Items from the TS Product and Service Catalogue where no changes are required to the TS Catalogue Item(s) and the lead time stated within the TS Product and Service Catalogue.;
TS Software	TS Specially Written Software, TS Supplier Software and TS Third Party Software;
TS Supplier Software	software which is proprietary to the Supplier (or an Affiliate of the Supplier) and which is or will be used by the Supplier for the purposes of providing the Transitional

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	Services, including the software specified as such in Annex 12 (<i>TS Software</i>);
TS Software Supporting Materials	has the meaning given in Paragraph 2.1(b) of Annex 32 (<i>TS Intellectual Property Rights</i>);
TS Specially Written Software	any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-contractor or other third party on behalf of the Supplier) specifically in connection with the Transitional Services, including any modifications or enhancements to TS Supplier Software or TS Third Party Software created specifically in connection with the Transitional Services;
TS Standards	the standards, policies and/or procedures identified in Annex 4 (<i>TS Standards</i>);
TS Technical Requirements	means the requirements as described in Appendix B –Technical Requirements to Annex 2 (<i>Transitional Services Description</i>);
TS Term	the period commencing on the Effective Date and ending on the date on which Milestone 17 is Achieved;
TS Termination Payment	has the meaning given in Paragraph 4.1 of Annex 16 (<i>Payments on TS Termination</i>);
TS Third Party Beneficiary	has the meaning given in Paragraph 41.1 (<i>TS Third Party Rights</i>) of this Schedule 34;
TS Third Party Contract(s)	a contract with a third party entered into by the Supplier exclusively for the purpose of delivering the Transitional Services, as listed in Annex 11 (<i>TS Third Party Contracts</i>);
TS Third Party COTS IPRs	TS Third Party IPRs that: (a) the Supplier makes generally available commercially prior to the date of this Contract (whether by way of sale, lease or licence) on standard

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

terms which are not typically
negotiated by the supplier save as to
price; and

(b) has a Non-trivial Customer Base;

**TS Third Party COTS
Software**

TS Third Party Software (including open
source software) that:

(a) the Supplier makes generally
available commercially prior to the
date of this Contract (whether by way
of sale, lease or licence) on standard
terms which are not typically
negotiated by the supplier save as to
price; and

(b) has a Non-trivial Customer base;

TS Third Party IPRs

Intellectual Property Rights owned by a third
party, but excluding Intellectual Property
Rights owned by the third party subsisting in
any TS Third Party Software, which in any
case is, will be or is proposed to be used by
the Supplier for the purposes of providing the
Transitional Services;

**TS Third Party Non-COTS
IPRs;**

TS Third Party IPRs that are not TS Third
Party COTS IPRs;

**TS Third Party Non-COTS
Software**

TS Third Party Software that is not TS Third
Party COTS Software;

TS Third Party Provisions

has the meaning given in Paragraph 41.1
(*TS Third Party Rights*) of this Schedule 34;

TS Third Party Software

software which is proprietary to any third
party (other than an Affiliate of the Supplier)
or any Open Source Software which in any
case is, will be or is proposed to be used by
the for the purposes of providing the
Transitional Services, including the software
specified as such in Annex 12 (*TS Software*);

**TS Time and Materials
Charges**

has the meaning given to it in Paragraph 4.8
of Annex 15 (*TS Charging and Invoicing*);

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

TS Unrecovered Costs	the costs incurred by the Transitional Supplier in the performance of the Transitional Services (as summarised in the TS Financial Model) to the extent that such costs are reasonable, proven and unavoidable and the same remain at the Termination Date to be recovered through TS Charges that but for the termination of the Transitional Services would have been payable by the Authority after the Termination Date in accordance with Annex 15 (<i>TS Charges and Invoicing</i>) as such costs and TS Charges are forecast in the TS Financial Model and Appendix 1 of Annex 16 (<i>Payments on TS Termination</i>);
TS Updates	in relation to any TS Software and/or any TS Deliverable means a version of such item which has been produced primarily to overcome TS Defects in, or to improve the operation of, that item;
TS Upgrades	any patch, TS New Release or upgrade of TS Software and/or a TS Deliverable, including standard upgrades, product enhancements, and any modifications, but excluding any TS Update which the Supplier or a third party software supplier (or any Affiliate of the Supplier or any third party) releases during the TS Term;
VVI Gateway Services	the gateway services, including the provision and management of the VVI Management Pod, being provided by the VVI Supplier pursuant to CCN number 005 entered into under the VVI Contract;
VVI Contract	the agreement for the provision of voice, video and network services entered into between the Authority and the Supplier dated 9 December 2021;
VVI Management Pod	means the VVI management pod described in Table 41 in Annex 8 (<i>Supplier TS Solution</i>);

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

VVI Supplier

means Vodafone Limited as the supplier of voice, video and network services, including the VVI Gateway Services, to the Authority under the VVI Contract.

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Part B: Definitions when applying Main Contract Provision

For the purposes of applying a Main Contract Provision in connection with the Transitional Services, the relevant capitalised expressions used in the relevant Main Contract Provision (as set out in Column 1 of the table below) shall be read as meaning or including (as appropriate) the relevant TS Definition (as defined in Part A of this Annex 1) set out in Column 2 of the table below:

Column 1 Defined term used in Main Contract Provision	Column 2 Relevant TS Definition
Assets	TS Assets
Authority Assets	Authority TS Assets
Authority Cause	Authority TS Cause
Authority Requirements	Authority TS Requirements
Authority Responsibilities	Authority TS Responsibilities
Catalogue Item	TS Catalogue Item
Certificate of Costs	Certificate of TS Costs
Change	TS Change
Charges	TS Charges
Commercially Sensitive Information	TS Commercially Sensitive Information
Contract Change	TS Contract Change
CPP Milestone	TS CPP Milestone

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Column 1 Defined term used in Main Contract Provision	Column 2 Relevant TS Definition
Critical Performance Failure	Critical TS Service Failure
Defect	TS Defect
Delay	TS Delay
Delay Payment	TS Delay Payment
Deliverable	TS Deliverable
Documentary Deliverable	TS Documentary Deliverable
Documentation	TS Documentation
Financial Model	TS Financial Model
IPRs Claim	TS IPRs Claim
IT Environment	TS IT Environment
ITSCM Plan	TS ITSCM Plan
Key Milestone	TS Key Milestone
Key Personnel	TS Key Personnel
Key Role	TS Key Role
Key Sub-contract	TS Key Sub-contract
Key Sub-contractor	TS Key Sub-contractor
Licensed Software	TS Licensed Software

SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)

Confidential
 Contract for the provision of WAN Services

Security Classification (Official)
 Contract reference: [REDACTED]

Column 1 Defined term used in Main Contract Provision	Column 2 Relevant TS Definition
Milestone	TS Milestone
Milestone Adjustment Payment Notice	TS Milestone Adjustment Payment Notice
Milestone Payment	TS Milestone Payment
New Release	TS New Release
Non-Documentary Deliverable	TS Non-Documentary Deliverable
Operational Change	TS Operational Change
Operational Service Commencement Date	Transitional Services Commencement Date
Performance Indicators	TS Performance Levels
Product and Service Catalogue	TS Product and Service Catalogue
Project	TS Project
Register	TS Register
Service Change	TS Service Change
Service Charge	TS Service Charge
Service Credits	TS Service Credits
Service Request	TS Service Request
Services Description	Transitional Services Description
Site(s)	any premises where any part of the Supplier TS System is located;

**SCHEDULE 34 (TRANSITIONAL SERVICES)
(ANNEX 1 TS DEFINITIONS)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Column 1 Defined term used in Main Contract Provision	Column 2 Relevant TS Definition
Specially Written Software	TS Specially Written Software
Supplier Background IPRs	TS Background IPRs
Supplier Software	TS Supplier Software
Software	TS Software
Supplier Solution	Supplier TS Solution
Supplier System	Supplier TS System
Target Performance Levels	TS Service Level Targets and TS KPI Targets
Term	TS Term
Termination Services	TS Termination Services
Third Party IPRs	TS Third Party IPRs
Third Party Software	TS Third Party Software
Update	TS Update
Upgrade	TS Upgrade

**ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 2
TRANSITIONAL SERVICES DESCRIPTION

**ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

TABLE OF CONTENTS

1 Definitions 3

2 Introduction 3

3 Objectives 3

4 Scope of The Transitional Services 4

5 Structure of Transitional Service Requirements 6

6 General principles 6

7 Design principles for the Transitional Services 7

8 Transitional Service Categories 8

APPENDICES 9

1 APPENDIX A (TS Service Management Requirements) 9

2 APPENDIX B (TS Technical Service Requirements) 9

**ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

1 DEFINITIONS

- 1.1 In this Annex, unless the context otherwise requires, capitalised expressions shall have the meanings set out in Annex 1 (*Definitions*).

2 INTRODUCTION

- 2.1 This Annex and its appendices detail the Transitional Services that shall be provided by the Supplier to the Authority.

- 2.2 The structure of this Annex is as follows:

Paragraph 3 describes the objectives for this document;

Paragraph 4 describes, at a summary level, the scope of the Transitional Services;

Paragraph 5 describes the structure, function and purpose of the requirements, the significance of each of the levels in the requirements and the purpose of the columns in the requirements tables;

Paragraph 6 sets general principles that need to underpin the Supplier's proposed solution to deliver the obligations set out in Appendices A and B of this Annex;

Paragraph 7 provides details of the design principles for the Transitional Services; and

Paragraph 8 provides the requirements in relation to each of the service aspects in:

a) Appendix A (*TS Service Management Requirements*); and

b) Appendix B (*TS Technical Service Requirements*); and

3 OBJECTIVES

- 3.1 The objectives of this Annex and its appendices are to:

3.1.1 define the scope of the Supplier's functions in respect of this Schedule 34 and in relation to the Authority;

3.1.2 provide key information about the Authority's requirements for the capabilities of the Supplier; and

**ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 3.1.3 establish responsibilities for the ongoing management and support of the Transitional Services.

4 SCOPE OF THE TRANSITIONAL SERVICES

- 4.1 The Supplier shall be responsible for the delivery, management and maintenance of the Transitional Services including (without limitation);

- 4.1.1 the management of the TS Gateway;
- 4.1.2 the management of IP Addressing; and
- 4.1.3 the technical integration of Transitional Services with Other Suppliers.

- 4.2 The Transitional Services shall include but not be limited to:

- 4.2.1 the provision of WAN infrastructure which shall securely inter-connect Sites to each other and the internet;
- 4.2.2 delivery of private VPN services in compliance with the PSN standards as set out in Annex 4 (*TS Standards*);
- 4.2.3 delivery of DIA services; and
- 4.2.4 integration Transitional Services, which shall include but not be limited to:
 - (a) ensuring compliance with TS Standards as set out in Annex 4 (*TS Standards*);
 - (b) the technical integration of telephony, video, and LAN services to ensure TS Service Levels are met;
 - (c) the design and management of the TS Gateway and IP addressing services as set out in Annex 8 (*Supplier TS Solution*) and Appendix B of this Annex.

- 4.3 The Supplier's role and responsibilities in delivering the Transitional Services include (without limitation):

- 4.3.1 all of the activities related to managing and supporting exit of the Transitional Services during the TS Term;
- 4.3.2 providing the Transitional Services in line with the TS Service Levels;

**ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 4.3.3 ensuring that Transitional Services, hardware and software are fully maintained and supported, subject to [REDACTED] of Appendix B (TS Technical Requirements) of this Annex 2 (Transitional Services Description);
 - 4.3.4 delivering a service that supports the provision to the Authority by Other Suppliers of a consistent End User experience across all End User Devices and all Authority Sites subject to the constraints of the design;
 - 4.3.5 implementing and maintaining elements and/or components of the Transitional Services in non-live environments;
 - 4.3.6 managing the delivery of installations, moves, additions, changes and disposals (IMACDs) across the Transitional Services and where services are delivered jointly with Other Suppliers; and
 - 4.3.7 provision of support and training for End Users where applicable, including but not limited to, guides and documentation for specified Transitional Services.
- 4.4 In the delivery of the Transitional Services, the Supplier shall at all times:
- 4.4.1 provide business as usual support to resolve incidents and problems through the provision of a support function which shall be integrated within the Authority's end to end service management processes and tooling suite and that aligns to ITIL. This support shall be delivered on site or remotely;
 - 4.4.2 work with the Authority and Other Suppliers in order to avoid service impacts to the End to End Services arising from changes, events or incidents to service and infrastructure components delivered by the Authority or Other Suppliers;
 - 4.4.3 provide programme, project and security management services for the elements of the End to End Services that are within the Supplier's scope; and

**ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

4.4.4 undertake pro-active and corrective maintenance of the Transitional Services, ensuring that all events, incidents and problems are resolved.

5 STRUCTURE OF TRANSITIONAL SERVICE REQUIREMENTS

5.1 The Transitional Service requirements listed in the Appendices to this Annex have been structured as follows:

Level 0	Header
Level 1	Relevant TS Service Line
Level 2	Process and function requirements of each TS Service Line
Level 3	Details of each requirement and the assignment of a unique requirement reference number

5.2 For example, the Service Strategy related requirements would be categorised as:

- level 0 = Service Strategy;
- level 1 = Demand Management
- level 2 = Analyse and Understand Patterns of Business Activity

For specific requirements an example would be:

- level 0 = Network Infrastructure Services;
- level 1 = Core Network Services;
- level 2 = IP Address Management.

5.3 The Supplier shall perform all obligations and fulfil all requirements outlined at level 3.

6 GENERAL PRINCIPLES

6.1 The Supplier shall have regard to the general principles set out in this Paragraph 6 in its delivery of the Transitional Services.

**ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 6.2 The Supplier shall identify in Annex 7 (*Authority TS Responsibilities*) any responsibilities of the Authority.
- 6.3 Subject to Paragraph 16.2 of Schedule 34, all services provided by the Supplier shall include TS Documentation including, but not limited to, operational documentation (such as the TS Service Operations Manual), technical documentation and operational diagrams and workflows.
- 6.4 Except as expressly stated in this Schedule 34, the Supplier shall provide support to the Authority where reasonably required to enable the Authority to maintain up-to-date service management policies, processes, and procedures in relation to the Transitional Services.
- 6.5 Where the Supplier proposes an update to the TS Service Operations Manual, the Authority shall review and decide whether to Approve the updated TS Service Operations Manual pursuant to the Document Approval Procedure in Part B of Schedule 13 (*Implementation*), having regard to the level, detail and scope of the TS Service Operations Manual and the required Transitional Services, and the Supplier will comply with the updated TS Service Operations Manual once Approved.
- 6.6 The Authority will monitor the Supplier's compliance with the TS Services Operations Manual and raise any non-compliances with the Supplier for addressing.

7 DESIGN PRINCIPLES FOR THE TRANSITIONAL SERVICES

- 7.1 The overarching design aim for the Authority is to create a single logical Network across all Sites within the TS IT Environment and which:
- 7.1.1 supports the delivery of the Transitional Services in accordance with TS Service Levels;
 - 7.1.2 provides effective and flexible management of capacity and change; and
 - 7.1.3 maximises business benefit and minimises business disruption for the Authority.

**ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 7.2 The Supplier shall ensure that the Transitional Services allow for the implementation of the Transitional Services in a modular and commoditised way, allowing for flexible and scalable Transitional Services that can be updated and replaced with minimal disruption of End to End Services.
- 7.3 The Supplier shall ensure that the Transitional Services facilitate process efficiency by choosing automation over manual intervention and empowering the business to self-serve.
- 7.4 The Supplier shall ensure that the Transitional Services maximise the contribution to the 'Greening government commitments' (as published and updated from time to time by the Department for Environment, Food and Rural Affairs) whilst minimising environmental impact.
- 7.5 The Supplier shall ensure that the Authority's business processes and objectives are understood and considered when designing and delivering Transitional Services.

8 TRANSITIONAL SERVICE CATEGORIES

- 8.1 The Transitional Service requirements have been categorised into TS Service Management Requirements (Appendix A) and TS Technical Service Requirements (Appendix B) and set out in each appendix in the levels outlined in Paragraph 5 above.
- 8.2 In Appendices A and B of this Annex, where capitalised level 1 and level 2 headings are used in the explanation of the level 3 requirements it is not the intention to observe these headings as defined terms, except where a relevant capitalised term is expressly defined in Schedule 1 of this Contract or Annex 1 of this Schedule 34.

**ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

APPENDICES

1 APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS)

See:

TS Service Management Requirements (Annex 2 Appendix A)

2 APPENDIX B (TS TECHNICAL SERVICE REQUIREMENTS)

See:

TS Technical Service Requirements (Annex 2 Appendix B)

End of Annex

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Annex 2 (Transitional Services Description)

Appendix A - TS Service Management Requirements

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

1 GENERAL REQUIREMENTS

1.1 General Principles

- 1.1.1 The Supplier shall take responsibility for delivery and management of the Transitional Services, including the interfacing and integration with the Authority and Other Suppliers.
- 1.1.2 In delivery of the Transitional Services, the Supplier shall adhere to the architecture standards as set out in Annex 4 (*TS Standards*).
- 1.1.3 The Supplier shall lead in a technical and/or service capacity where the delivery of any Transitional Service for which the Supplier is responsible requires the support from one or more Other Suppliers.
- 1.1.4 General principles against which the Service Requirements are to be delivered are listed below:

Requirement No.	Level	Requirement
	2	General Requirements
	3	The Supplier shall provide, maintain, and support the Transitional Services to all Sites identified by the Authority.
1.1.4.1	3	The Supplier shall ensure, interoperability and connectivity to and between ITIL V3 and other service management best practices within the ITSM Framework.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
1.1.4.2	3	The Supplier shall create an 'Open Standards Exemption Report' for any solution or solution component where the Authority agrees non-compliance with the Open Standards Principles (see Paragraph 10.2 of Annex 4 (TS Standards), and provide this to the Authority within twenty (20) Working Days of the Authority's agreement to non-compliance.
1.1.4.3	3	The Supplier shall, unless otherwise agreed with the Authority, ensure that all solutions and solution components shall meet the functional needs of the Authority and comply with Open Standard principles where they exist.
1.1.4.4	3	The Supplier shall create an Open Standards alignment report as required and provide this to the Authority within thirty (30) Working Days of the anniversary of the Effective Date for Approval.
1.1.4.5	3	The Supplier shall, as required under health and safety regulations, perform electrical safety checks on Devices used for the provision of the Transitional Services which reside within local server room(s) and cabinets located outside the local server room(s) at Authority Sites.
1.1.4.6	3	The Supplier shall maintain, manage and support the Transitional Services to minimise where possible attendance at Authority Sites.
1.1.4.7	3	The Supplier shall be responsible for the implementation and provisioning of the Transitional Services in accordance with the current designs agreed by the Authority.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
1.1.4.8	3	The Supplier shall design and manage the Transitional Services to support the delivery of the Transitional Services in accordance with Annex 3 (<i>TS Performance Levels</i>).
1.1.4.9	3	The Supplier shall implement and provision the Transitional Services to support the delivery of Transitional Services in accordance with Annex 3 (<i>TS Performance Levels</i>).
1.1.4.10	3	The Supplier shall work and collaborate with the Authority to create a sustainability report covering the previous six (6) months' progress against applicable requirements and targets as set out in the agreed TS Service Operations Manual.
1.1.4.11	3	The Supplier shall identify an appropriately qualified ICT sustainability Single Point of Contact (" SPoC ") and inform the Authority within two (2) months of the Effective Date of who that is. The ICT Sustainability SPoC shall be responsible for all aspects of ICT Sustainability related to the delivery of the Transitional Services during the TS Term.
1.1.4.12	3	The Supplier shall ensure continuity in the identified ICT sustainability SPoC throughout the TS Term.
1.1.4.13	3	The Supplier shall create a sustainable ICT improvement plan, for any area where ICT maturity is assessed as being lower than level 3 against the HMG Green ICT Maturity Assessment Model, as detailed in the Greening Government ICT Strategy (" The Sustainable ICT Improvement Plan "). The Sustainable ICT Improvement Plan shall detail how the Supplier shall reach level 3 maturity or higher, and shall be submitted within two (2) months of the Supplier completing the assessment for Approval.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
1.1.4.14	3	The Supplier shall, for any actions identified by the Sustainable ICT Improvement Plan that are agreed by the Authority, implement these actions within the timescales set out within the Sustainable ICT Improvement Plan.

2 TS PROJECT DELIVERY MANAGEMENT

2.1 TS Project Management

- 2.1.1 TS Project Management is a critical activity within TS Project Delivery Management and aims to ensure appropriate TS Project Management skills and resources are available as and when required by the Authority.
- 2.1.2 The TS Project Management requirements describe the responsibilities of the Supplier with regards to a consistent approach to, and governance of, all stages of a project's lifecycle in accordance with industry leading methodologies as defined in Annex 4 (*TS Standards*).
- 2.1.3 The main objectives for TS Project Management are to:
 - (a) provide the Authority with an accessible mechanism to supplement existing skills and resources on an ad hoc basis to address the variable needs of the business;
 - (b) ensure a consistent approach to project management is adopted by all Other Suppliers to drive a more integrated governance and delivery capability;
 - (c) assure compliance to the relevant processes, procedures and standards set out in the agreed TS Service Operations Manual; and
 - (d) ensure a consistent approach to the delivery of new Transitional Services.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

2.1.4 The General Requirements for TS Project Management are listed below:

Requirement No.	Level	Requirement
	2	General Requirements
2.1.4.1	3	The Supplier shall provide and maintain a TS Project Management service which is aligned to industry leading methodologies and aligned to the relevant standards set out in Annex 4 (<i>TS Standards</i>).
2.1.4.2	3	The Supplier shall at all times, work in accordance with the TS Project Management processes and procedures as set out in this Annex 2 Appendix A and the agreed TS Service Operations Manual.
2.1.4.3	3	The Supplier shall work and collaborate with the Authority in any review as a result of the Supplier's non-compliance with the TS Project Management processes and procedures as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Authority.
2.1.4.4	3	The Supplier shall, where such information has not been provided within Annex 15 (<i>TS Charges and Invoicing</i>), provide a rate card for TS Project Management services in line with the Skills Framework for the Information Age (SFIA) to the Authority for approval within 40 Working Days of the Effective Date.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

3 SERVICE STRATEGY

3.1 TS Demand Management

- 3.1.1 TS Demand Management is a critical activity within Service Management. TS Demand Management aims to manage the uncertainty in business demand for the Transitional Services and ensure the appropriate capacity of the Transitional Service is available as and when required by the Authority.
- 3.1.2 The TS Demand Management process aims to understand the Authority's consumption levels for the Transitional Services and how these vary over the business cycle, with the aim of ensuring the provision of an appropriate level of service to support the Authority's need.
- 3.1.3 The benefit of effective TS Demand Management is:
 - (a) the design for Transitional Services is optimised to meet the Patterns of Business Activity (PBA) they support;
 - (b) effective management of the TS Produce and Service Catalogue by mapping demand to the appropriate Transitional Services;
 - (c) informs investment decisions; and
 - (d) informs resource scheduling and management.
- 3.1.4 The Service Requirements for TS Demand Management are listed below:

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	General Requirements
3.1.4.1	3	The Supplier shall at all times, work in accordance with the TS Demand Management processes as set out in the agreed TS Service Operations Manual.
3.1.4.2	3	The Supplier shall work and collaborate with the Authority in any review as a result of the Supplier's non-compliance with the TS Demand Management processes as set out in the agreed TS Service Operations Manual, and implement any required corrective action that has been agreed by the Authority.
	2	Analyse and Understand Patterns of Business Activity
3.1.4.3	3	The Supplier shall support the Authority in performing service activity based analysis.
	2	Define, Match and Report on WAN/Gateway services
3.1.4.4	3	The Supplier shall support the Authority by compiling Transitional Service forecasts for each Service Measurement Period set out in the agreed TS Service Operations Manual.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Develop Service Packages
3.1.4.5	3	The Supplier shall support the Authority in making recommendations on changes or improvements to the composition of Transitional Service packages for the Transitional Services, including appropriate TS Service Levels.

3.2 TS Financial Management

- 3.2.1 The TS Financial Management process shall provide the Authority with the quantification of the value of the Transitional Services provided by the Supplier and consumed by the Authority in financial terms (subject to all restriction and limitations applied with regards to sharing of financial information with the Authority under this Contract).
- 3.2.2 The TS Financial Management service is required to ensure that the Authority only pays for the Transitional Services that are consumed, or which they are obligated to pay for in line with appropriate commercial agreements.
- 3.2.3 The benefit of TS Financial Management is that it helps and supports the Authority in being able to:
 - (a) inform decision making to enable the achievement of stated ICT 'run and maintain' savings;
 - (b) determine the size, scope and complexity of the portfolio of TS Services;
 - (c) ensures financial compliance and control;

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (d) apportion charges appropriately;
- (e) maintain operational cost control; and
- (f) conduct service lifecycle investment analysis.

3.2.4 The Service Requirements for TS Financial Management are listed below:

Requirement No.	Level	Requirement
	2	General Requirements
3.2.4.1	3	The Supplier shall work in accordance with the TS Financial Management processes as set out in the agreed TS Service Operations Manual.
3.2.4.2	3	The Supplier shall work and collaborate with the Authority in any review required as a result of the Supplier's non-compliance with the TS Financial Management processes as set out in the agreed TS Service Operations Manual, and implement any required corrective action that has been agreed by the Authority.
3.2.4.3	3	The Supplier shall provide TS Financial Management for the Transitional Services as set out in this Annex 2 Appendix A and the agreed TS Service Operations Manual.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Validate Service Consumption
3.2.4.4	3	The Supplier shall provide all relevant Transitional Services consumption information to the Authority in order that Transitional Services usage can be verified by the Authority for the purposes of the TS Financial Management processes as set out in the agreed TS Service Operations Manual.
3.2.4.5	3	In support of invoices submitted by the Supplier in accordance with the Annex 15 (<i>TS Charges and Invoicing</i>), the Supplier shall provide all relevant Transitional Service consumption information and any applicable TS Service Credits to the Authority. .
3.2.4.6	3	In the event that the Authority identifies discrepancies between the Transitional Service consumption information and any applicable TS Service Credits provided by the Supplier, the Supplier shall work and collaborate with the Authority to resolve such discrepancies.
	2	Forecasting and Business Case support
3.2.4.7	3	The Supplier shall provide relevant financial information in a timely manner to input into detailed Business Cases for Changes to the Transitional Services.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
3.2.4.8	3	The Supplier shall support the Authority with financial forecasting in respect of the Transitional Services in support of the Authority's budgeting process.
	2	Request to Pay
3.2.4.9	3	The Supplier shall support the Authority in the requisitioning of Transitional Services in the fulfilment of TS Service Requests.

3.3 TS Service Portfolio Management

- 3.3.1 TS Service Portfolio Management is the process for managing the portfolio of Transitional Services and ensuring that business value is achieved across the Transitional Services provided to the Authority.
- 3.3.2 TS Service Portfolio Management provides the overall governance in the identification, provision of, delivery and retirement of the Transitional Services provided by the Supplier. The Supplier shall work with the Authority in providing the Service Portfolio service and will identify and present to the Authority suggestions for the transition, improvement, refresh and retirement of the Transitional Services.
- 3.3.3 The benefit of TS Service Portfolio Management to the Authority is demonstrated through the ability to anticipate change while maintaining traceability to the Authority's overarching ICT strategy and planning by:
 - (a) providing the means to characterise service investments; and

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) providing an essential link between business portfolio management (demand pipeline) and IT project and programme portfolio management.

3.3.4 The Service Requirements for TS Service Portfolio Management are listed below:

Requirement No.	Level	Requirement
	2	General Requirements
3.3.4.1	3	The Supplier shall at all times, work in accordance with the TS Service Portfolio processes as set out in the agreed TS Service Operations Manual.
3.3.4.2	3	The Supplier shall work and collaborate with the Authority in any review as a result of the Supplier's non-compliance with the TS Service Portfolio Management processes and procedures as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Authority.
3.3.4.3	3	The Supplier shall provide TS Service Portfolio Management for the Transitional Services as set out in this Annex 2 Appendix A and the agreed TS Service Operations Manual.
	2	Define the TS Service Portfolio
3.3.4.4	3	The Supplier shall produce, maintain and provide to the Authority details of the TS Service Portfolio for the Transitional Services it provides.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

3.4 TS Risk Management

- 3.4.1 The TS Risk Management process needs to be aligned with the Authority's strategic risk management approach and contain the following steps across the Transitional Service delivery lifecycle.
- (a) identification and assessment of exposure to risk and subsequent impacts;
 - (b) application of appropriate controls to manage exposure and impact;
 - (c) ensure communication of mitigating actions; and
 - (d) management of risk is performed within a transparent, repeatable and consistent process.
- 3.4.2 TS Risk Management supports the decision-making process by being able to accurately assess risks and the associated impacts and potential benefits of actions in relation to the ability to support and deliver Transitional Services.
- 3.4.3 Effective TS Risk Management enables the identification of positive and negative risks to be analysed and a course of action to be determined based on value and impact to the Transitional Service delivery lifecycle, ensuring that the best possible outcome can be achieved.
- 3.4.4 The Service Requirements for TS Risk Management are listed below:

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	General Requirements
3.4.4.1	3	The Supplier shall at all times, work in accordance with the TS Risk Management processes as set out in the agreed TS Service Operations Manual.
3.4.4.2	3	The Supplier shall work and collaborate with the Authority in any review as a result of the Supplier's non-compliance with the TS Risk Management Processes as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Authority.
3.4.4.3	3	The Supplier shall support TS Risk Management for the Transitional Services as set out in this Annex 2 Appendix A and the agreed TS Service Operations Manual.
	2	Risk Identification and Capture
3.4.4.4	3	The Supplier shall support the Authority in the identification, analysis and management of risks across the Transitional Service delivery lifecycle in accordance with the TS Risk Management processes and procedures as set out in the agreed TS Service Operations Manual.
3.4.4.5	3	The Supplier shall support the Authority in making TS Risk Management information available to the Authority.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Risk Monitoring
3.4.4.6	3	The Supplier shall conduct proactive monitoring to identify any emergent risk to the provision of Transitional Services and where possible End to End Services and report these immediately to the Authority.
	2	Risk Reporting
3.4.4.7	3	The Supplier shall attend risk review boards, develop and manage risk action plans and recommend to the Authority appropriate measures to mitigate any risk identified.
3.4.4.8	3	Where requested by the Authority, the Supplier shall implement the measures identified in answer to an emerging risk which has been approved by the Authority within twenty (20) Working Days of approval being granted.

4 TS SERVICE DESIGN

4.1 The purpose of the Service Design phase is to ensure that the design and development of the Transitional Services deliver value to the Authority.

4.2 TS Availability Management

4.2.1 The Transitional Service must include the following steps in the TS Availability Management lifecycle:

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (a) design for availability;
 - (b) monitor, measure and report availability; and
 - (c) manage risk to availability.
- 4.2.2 The purpose of TS Availability Management is to define, analyse, plan, measure and improve all aspects of the availability of IT Environments, systems and Transitional Services. TS Availability Management is responsible for ensuring that all IT infrastructures, processes, tools and resources are appropriate for the agreed availability targets.
- 4.2.3 The benefit of TS Availability Management is that the process ensures that the availability of systems and services matches the evolving agreed needs of the business. The availability and reliability of IT Environments, systems and services can directly influence customer satisfaction and the reputation of the business.
- 4.2.4 The Service Requirements for TS Availability Management are listed below:

Requirement No.	Level	Requirement
	2	General Requirements
4.2.4.1	3	The Supplier shall at all times, work in accordance with the TS Availability Management processes and procedures as set out in the agreed TS Service Operations Manual.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
4.2.4.2	3	The Supplier shall ensure that any TS Availability Management Information System (" TS AMIS ") that they use interfaces effectively with the TS AMIS provided by the Authority in accordance with the relevant TS Availability Management processes and procedures as set out in the agreed TS Service Operations Manual.
4.2.4.3	3	The Supplier shall work and collaborate with the Authority in any review required as a result of the Supplier's non-compliance with the TS Availability Management processes and procedures as set out in the agreed TS Service Operations Manual, and implement any required corrective action that has been agreed by the Authority.
4.2.4.4		The Supplier shall provide TS Availability Management for the Transitional Services, as set out in this Annex 2 Appendix A and the agreed TS Service Operations Manual.
	2	Plan and Design Availability
4.2.4.5	3	The Supplier shall provide and deliver the Transitional Services to the agreed availability, design criteria and TS Service Levels, for Transitional Services or changed Transitional Services in accordance with Schedule 22 (<i>Change Control Procedure, Service Requests and Projects</i>).

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
4.2.4.6	3	The Supplier shall support the Authority in producing and updating the Availability Plan every Service Period in accordance with the TS Availability Management processes and procedures as set out in the agreed TS Service Operations Manual.
	2	Assess and Manage Risk to Availability
4.2.4.7	3	The Supplier shall actively participate in availability risk reviews carried out on the Transitional Services by the Authority.
	2	Monitor, Measure, Analyse, Report, and Review Availability
4.2.4.8	3	The Supplier shall work and collaborate with the Authority to schedule and manage any planned downtime in order to minimise disruption to normal business operations.
4.2.4.9	3	The Supplier shall provide to the Authority planned downtime information in accordance with the TS Availability Management processes as set out in the agreed TS Service Operations Manual.
4.2.4.10	3	The Supplier shall provide Availability data to the Authority in accordance with the TS Availability Management processes as set out in the agreed TS Service Operations Manual.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
4.2.4.11	3	The Supplier shall gather, and deliver, to the Authority the data as set out in the agreed TS Service Operations Manual.
	2	Investigate and Implement Measures to Improve Availability Performance
4.2.4.12	3	The Supplier shall produce for the Authority service component failure impact analysis information within each Service Measurement Period in accordance with the TS Availability Management processes as set out in the agreed TS Service Operations Manual and propose to the Authority possible mitigation actions to avoid future degradation of the availability of the Transitional Services or components thereof.

4.3 TS Capacity Management

4.3.1 The Supplier shall include the following sub-processes within the Capacity Management lifecycle:

- (a) Services Capacity Management; and
- (b) Services Capacity Management Reporting.

4.3.2 The purpose of TS Capacity Management is to ensure that the capacity of the Transitional Services and the supporting IT Environment, systems and services is able to deliver the agreed TS Service Levels in an efficient and timely manner.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

4.3.3 The benefit of TS Capacity Management is that it is responsible for ensuring that resources are planned and scheduled to provide a consistent level of service that is matched to the needs of the Authority. TS Capacity Management provides a capacity plan that outlines the resources needed to support the required business outcomes (the “**TS Capacity Plan**”).

4.3.4 The Service Requirements for TS Capacity Management are listed below:

Requirement No.	Level	Requirement
	2	General Requirements
4.3.4.1	3	The Supplier shall at all times, work in accordance with the TS Capacity Management processes and procedures as set out in the agreed TS Service Operations Manual.
4.3.4.2	3	The Supplier shall support the Authority in the production and maintenance of a TS Capacity Plan by providing the Authority with capacity plans for the Transitional Services and components which it is providing.
4.3.4.3	3	The Supplier shall work and collaborate with the Authority in any review as a result of the Supplier’s non-compliance with the TS Capacity Management processes as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Authority.
4.3.4.4	3	The Supplier shall provide TS Capacity Management for the Transitional Services as set out in this Annex 2 Appendix A and the agreed TS Service Operations Manual.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Review Current Capacity
4.3.4.5	3	Following receipt of the quarterly business forecast from the Authority, and in accordance with the TS Capacity Management processes as set out in the agreed TS Service Operations Manual, the Supplier shall: (i) update the Services Capacity Plan to include those future volumes; and (ii) submit their Capacity Plan to the Authority.
4.3.4.6	3	The Supplier shall provide Capacity information required by the Authority as set out in the agreed TS Service Operations Manual.
	2	Assess and Document Capacity Requirements
4.3.4.7	3	The Supplier shall support the Authority to model any proposed TS Change and the consumption trends in the Transitional Services in order to identify any TS Change that needs to be made to current Transitional Services or components thereof to ensure that the TS Service Levels are achieved.
4.3.4.8	3	The Supplier shall manage the availability of appropriate resources units to meet the predicted demands to the Transitional Services.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
4.3.4.9	3	The Supplier shall support the Authority in monitoring and reporting on the Transitional Services against the agreed Capacity thresholds as set out in the agreed TS Service Operations Manual.
4.3.4.10	3	The Supplier shall monitor and report the Transitional Services, as agreed with the Authority, against the agreed Capacity thresholds and notify the Authority as soon as they become aware of any Capacity issues or potential Capacity issues.
4.3.4.11	3	The Supplier shall continually monitor and report recommendations for optimisation of Capacity by increasing or decreasing Capacity in accordance with the TS Capacity Management Processes as set out in the agreed TS Service Operations Manual in order for the Transitional Service to maintain the operation of the Transitional Services in accordance with Annex 3 (<i>TS Performance Levels</i>).
4.3.4.12	3	The Supplier shall produce and submit a capacity report for the Transitional Services they are providing to the Authority in accordance with the TS Capacity Management Processes as set out in the agreed TS Service Operations Manual for each Service Period comparing the actual volumes provided against the volumes forecasted in their TS Capacity Plan.
4.3.4.13	3	The Supplier shall produce and submit to the Authority a 'Quarterly Capacity Plan' in accordance with the TS Capacity Management processes as set out in the agreed TS Service Operations Manual.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

4.4 TS IT Service Continuity Management

- 4.4.1 TS IT Service Continuity Management (TS ITSCM) shall support the overall Authority’s business continuity management process by ensuring that the required IT technical and service facilities (including computer systems, networks, applications, data repositories, telecommunications, environment, technical support and Service Desk) can be resumed within required and agreed business timescales.
- 4.4.2 TS ITSCM shall support the Authority’s business continuity planning process and ensure that the recovery arrangements for designated Transitional Services and components thereof are aligned to identified and agreed business impacts, risks and needs.
- 4.4.3 TS ITSCM manages the risks that could materially impact the performance and availability of the Transitional Services as part of the End to End Services. TS ITSCM ensures that Transitional Services can be provided in accordance with agreed TS Service Levels.
- 4.4.4 The Service Requirements for TS IT Service Continuity Management are listed below:

Requirement No.	Level	Requirement
	2	General Requirements
4.4.4.1	3	The Supplier shall at all times, work in accordance with the TS ITSC Management processes as set out in the agreed TS Service Operations Manual.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
4.4.4.2	3	The Supplier shall provide the Authority with a SPoC for the ITSCM Plan and provide an escalation process with full contact details. The SpoC shall be identified as a TS Key Person as set out in Annex 29 (<i>TS Key Personnel</i>).
4.4.4.3	3	The Supplier shall support the TS ITSCM planning process ensuring its ITSCM Plan aligns to the Authority's IT service continuity management plan.
4.4.4.4	3	The Supplier shall develop and maintain an up-to-date ITSCM Plan for the Transitional Services that is consistent and conformant with Schedule 26 (<i>Service Continuity Plan</i>) and the agreed TS Service Operations Manual, and provide a copy of its ITSCM Plan to the Authority.
4.4.4.5	3	The Supplier shall provide TS ITSC awareness and training for all the TS Supplier Personnel relevant to TS ITSCM within three (3) months of the Effective Date.
4.4.4.6	3	The Supplier shall work and collaborate with the Authority in any review required as a result of the Supplier's non-compliance with the ITSCM processes as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Authority.
4.4.4.7	3	The Supplier shall provide TS IT Service Continuity Management for the Transitional Services in accordance with Schedule 26 (<i>Transitional Service Continuity Plan</i>).

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
4.4.4.8	3	The Supplier shall ensure that all Business Impact Analysis communicated by the Authority are factored into its ITSCM Plan(s) for the Transitional Services it provides.
4.4.4.9	3	The Supplier shall support the Authority in undertaking an annual review, or a review post invocation, of the ITSCM Plan and associated processes.
	2	TS ITSCM Testing
4.4.4.10	3	The Supplier shall participate in the ITSCM test exercise regime and undertake the relevant activities in compliance with Schedule 26 (<i>Service Continuity Plan</i>).
4.4.4.11	3	The Supplier shall review the draft TS ITSCM testing schedule (" TS ITSCM Testing Schedule ") provided by the Authority and shall submit information and assistance as required by the Authority.
4.4.4.12	3	The Supplier shall comply with the TS ITSCM Testing Schedule and the relevant TS ITTSC Management procedures at all times.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
4.4.4.13	3	The Supplier shall, when they have executed tests defined under the TS ITSCM Testing Schedule for the Transitional Services, provide the Authority with the appropriate TS ITSCM Test Reports and remediation plans including a possible retest to resolve failed tests.
	2	TSITSCM Plan Invocation
4.4.4.14	3	The Supplier shall define with the Authority clear and unambiguous triggers and closure points relating to TS IT Service Continuity (TS ITSC) Events.
4.4.4.15	3	The Supplier shall notify the Authority of the occurrence of any TS ITSC Event and shall provide formal recommendations for invoking the relevant ITSC Plan(s) to ensure that the Transitional Services are delivered with the agreed recovery objectives and in accordance with Annex 3 (<i>TS Performance Levels</i>).
4.4.4.16	3	Following notice from the Authority that it requires an ITSCM Plan(s) to be invoked, the Supplier shall comply and immediately launch the applicable ITSCM Plan(s).
4.4.4.17	3	Following the agreed closure of an TS ITSC Event, the Supplier involved in the execution of the ITSC Plan shall provide the Authority with such information, guidance and assistance as may be reasonably requested by the Authority to support in the production of a TS ITSC Event report.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	TS ITSCM Reviews
4.4.4.18	3	The Supplier shall support the Authority in ensuring there is appropriate monitoring and review of the ITSCM Plans in accordance with the relevant TS ITSC Management Procedures as defined in the agreed TS Service Operations Manual

4.5 TS Product and Service Catalogue Management

- 4.5.1 TS Catalogue Management provides a single source of consistent information on all Transitional Services.
- 4.5.2 The TS Catalogue Management process shall ensure that the Authority has an accurate TS Product and Service Catalogue produced and maintained for all the Transitional Services.
- 4.5.3 TS Catalogue Management shall provide a central source of information on the Transitional Services delivered by the Supplier. The TS Product and Service Catalogue shall provide an accurate, consistent picture of all the Transitional Services available.
- 4.5.4 The TS Requirements for TS Catalogue Management are listed below:

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Require ment No.	Level	Requirement
	2	General Requirements
4.5.4.1	3	The Supplier shall at all times, work in accordance with the TS Catalogue Management processes set out in the agreed TS Service Operations Manual.
4.5.4.2	3	The Supplier shall work and collaborate with the Authority in any review as a result of the Supplier's non-compliance with the TS Catalogue Management processes as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Authority.
4.5.4.3	3	The Supplier shall provide TS Catalogue Management for the Transitional Services as set out in this Annex 2 Appendix A and the agreed TS Service Operations Manual.
	2	Agree Service Content and Definition
4.5.4.4	3	The Supplier shall update and contribute to the production of the TS Product and Service Catalogue.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Require ment No.	Level	Requirement
	2	Manage and Maintain the TS Product and Service Catalogue
4.5.4.5	3	The Supplier shall maintain their elements of the TS Product and Service Catalogue in accordance with the Request Fulfilment processes as set out in the agreed TS Service Operations Manual to ensure that they are always current with the Transitional Services.
4.5.4.6	3	The Supplier shall support the development and maintenance of a subset of the TS Product and Service Catalogue so that it is available to the Authority.
4.5.4.7	3	The Supplier shall agree and document service definitions and all relevant documentation with the Authority for Transitional Services and components thereof listed in the TS Product and Service Catalogue.
4.5.4.8	3	The Supplier shall ensure that all Transitional Services and components thereof listed in their TS Produce and Service Catalogue have appropriate TS Assets and TS Configuration Items ("CIs") identified within the Configuration Management System managed by the Authority.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

4.6 TS Service Level Management

4.6.1 The TS Service Level Management process ensures that the agreed level of service is provided for all Transitional Services and that all future Transitional Services are delivered to agreed achievable targets. TS Service Level Management shall demonstrate the following steps within the Service Level Management lifecycle:

- (a) design and development of TS Service Levels for all Transitional Services provided by the Supplier;
- (b) analyse, determine, document and agree business requirements for a Transitional Service and produce and document Service Level Requirements for Approval by the Authority;
- (c) ensure that appropriate arrangements are agreed and implemented that support the provision of the Transitional Services to agreed TS Service Levels and that these are aligned and consistent with those set out in the Annex 3 (*TS Performance Levels*);
- (d) implement Service TS Levels upon Approval;
- (e) monitor Transitional Service performance against the TS Service Levels and produce and communicate regular performance reports;
and
- (f) perform regular Transitional Service reviews.

4.6.2 TS Service Level Management is a vital process responsible for ensuring that:

- (a) negotiated and agreed TS Service Levels for the Transitional Services from the Supplier and Other Suppliers are satisfactorily met;
- (b) back to back arrangements between the Supplier, and Other Suppliers and supporting ITSM processes are appropriate and proportionate for the agreed TS Service Levels;
- (c) monitoring and reporting on TS Service Levels is performed; and

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

(d) the Authority is regularly informed and engaged on performance of all TS Service Levels.

4.6.3 TS Service Level Management shall provide a consistent interface to the Authority for all Transitional Service-related issues. It shall provide the Authority with the agreed TS Service Levels and the required management information to monitor that those targets have been met. Where targets are breached, TS Service Level Management should provide feedback on the cause of the breach and details of the actions taken to prevent the breach from reoccurring, thus providing a reliable communication channel and trusted relationship with the Authority’s representatives.

4.6.4 The Service Requirements for TS Service Level Management are listed below:

Requirement No.	Level	Requirement
	2	General Requirements
4.6.4.1	3	The Supplier shall ensure that the Transitional Services are delivered in accordance with Annex 3 (<i>TS Performance Levels</i>).
4.6.4.2	3	The Supplier shall at all times work in accordance with the TS Service Level Management processes and procedures as set out in the agreed TS Service Operations Manual.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
4.6.4.3	3	The Supplier shall work and collaborate with the Authority in any review required as a result of the Supplier's non-compliance with the Annex 3 (<i>TS Performance Levels</i>) and implement any required corrective action that has been agreed by the Authority.
	2	New Transitional Services
4.6.4.4	3	The Supplier shall provide and deliver the Transitional Services to the agreed availability, design criteria and TS Service Levels for new or changed Transitional Services in accordance with Schedule 22 (<i>Change Control Procedure, Service Requests and Projects</i>).
4.6.4.5	3	The Supplier shall support the Authority in managing, monitoring, measuring and reporting on the performance of the Transitional Services and the TS Service Levels.
4.6.4.6	3	The Supplier shall support the Authority to ensure that all TS Service Levels are met in accordance with the TS Service Levels set out in Annex 3 (<i>TS Performance Levels</i>).

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Document and Agree TS Service Levels
4.6.4.7	3	The Supplier shall support the Authority in the creation of TS Service Levels for the Transitional Services and where possible End to End Services.
	2	Activate TS Service Level
4.6.4.8	3	The Supplier shall capture, collate and make available to the Authority all information relevant to TS Service Levels for the Transitional Services they provide in accordance with Annex 3 (<i>TS Performance Levels</i>) and to make this information available to the Authority both in real time and as per the Service Measurement Period set out in Annex 3 (<i>TS Performance Levels</i>).
	2	Agree Reporting Framework
4.6.4.9	3	The Supplier shall support the Authority in the analysis of data in provision of performance measurement information.
4.6.4.10	3	The Supplier shall support the Authority in reviewing failures and/or threatened breaches of TS Service Levels for the Transitional Services and agree the content of an Exception Report including a proposed Recovery Plan or Rectification Plan in accordance with the requirements set out in Annex 3 (<i>TS Performance Levels</i>).

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
4.6.4.11	3	The Supplier shall support the Authority in the development of a Systems of Measurement Reference Document for all of the Transitional Services that contribute to the TS Service Levels set out in Annex 3 (<i>TS Performance Levels</i>).
4.6.4.12	3	The Supplier shall attend and actively participate in Supplier performance reviews with the Authority in accordance with Schedule 21 (<i>Governance</i>) to assess and review performance of the Transitional Services against performance criteria set out in Annex 3 (<i>TS Performance Levels</i>).

4.7 TS Supplier Management

- 4.7.1 The TS Supplier Management requirements contain the responsibilities of the Supplier in support of the Authority in monitoring and reviewing the performance and engagement of the Supplier in complying with obligations to the policies and procedures set down by the Authority and their contracted obligations agreed with the Authority.
- 4.7.2 The main objectives for the TS Supplier Management process are:
- (a) work with the Authority to ensure conformance and adherence to agreed procedures;
 - (b) manage the take on of new suppliers;
 - (c) manage the non-compliance to Policies and Procedures by the Supplier;
 - (d) manage the day-to-day operational relationship with suppliers;
 - (e) conduct regular performance reviews with suppliers; and

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (f) provide an interface for formal communications from suppliers and the Authority.
- 4.7.3 This is a valuable process to the Authority as it ensures that the day-to-day engagement with the Supplier is managed to ensure that all suppliers operate to a common understanding and performance level.
- 4.7.4 The Supplier shall provide a single point of contact for the Transitional Services to the Authority.
- 4.7.5 The Service Requirements for TS Supplier Management are listed below:

Requirement No.	Level	Requirement
	2	General Requirements
4.7.5.1	3	The Supplier shall work and collaborate with Other Suppliers to support the Authority in delivering the Transitional Services in compliance with the TS Service Levels set out in Annex 3 (<i>TS Performance Levels</i>).
4.7.5.2	3	The Supplier shall at all times, work in accordance with the TS Supplier Management processes as set out in the agreed TS Service Operations Manual.
4.7.5.3	3	The Supplier shall work and collaborate with the Authority in any review as a result of the Supplier's non-compliance with the TS Supplier Management processes as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Authority.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Management of the Transitional Services
4.7.5.4	3	The Supplier shall provide all relevant information and support to the Authority on Transitional Services, agreed standards and performance targets.
4.7.5.5	3	The Supplier shall attend and actively participate in regular Supplier performance reviews convened by the Authority in accordance with Schedule 21 (<i>Governance</i>).
4.7.5.6	3	The Supplier shall support the Authority by attending regular performance reviews on the Transitional Services and agreed process improvement plans.
4.7.5.7	3	The Supplier shall support the Authority to establish a supplier scorecard.
4.7.5.8	3	The Supplier shall provide appropriate performance information as requested by the Authority in support of the production of a regular supplier scorecard.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Supply Chain Risk Management
4.7.5.9	3	The Supplier shall support the Authority in the management and maintenance of risks to the Transitional Service supply chain.
4.7.5.10	3	The Supplier shall participate in and provide support to any review of risks where participation has been requested by the Authority.

5 TS SERVICE TRANSITION

5.1 Introduction

5.1.1 The purpose of the Transition phase of the Service Delivery lifecycle is to plan and coordinate resources to ensure that the requirements derived from the Service Design phase are effectively realised in Service Operations.

5.2 Transition Planning and Support

5.2.1 The Supplier shall ensure that the service for the introduction of approved new or changed Transitional Services has the following activities embedded across the Transition Planning and Support lifecycle:

- (a) prepare for and plan for transition;
- (b) ensure Service Design packages are created for new or changed Transitional Services;

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (c) identify, manage and limit the risks to service interruption;
- (d) complete Transitional Service requirements capture;
- (e) complete Service Design for new or changed Transitional Services;
- (f) confirm Service Design with the approval body;
- (g) complete Transitional Service validation Testing;
- (h) confirm Transitional Service release and deployment readiness; and
- (i) perform Transitional Service handover and review.

5.2.2 The main purpose of Transition Planning and Support is to coordinate the resources required to ensure specifications for the design of a new or changed Transitional Service are realised. This is achieved through the use of a consistent and repeatable framework for the evaluation of Transitional Service capability and risk before a new or changed Transitional Service is deployed.

5.2.3 The benefit of an effective and efficient Transition Planning and Support process is that it enables projects to estimate and understand costs, timings and resource requirements, with associated risks of transition in to live. This enables:

- (a) higher volumes of successful TS Change;
- (b) improved expectation setting for all stakeholders;
- (c) increased confidence in the new or changed Transitional Service shall be maintained and supported within a cost-effective manner where there are no unexpected operational costs associated to the live running of the service;
- (d) better management of the risks in transitioning new or changed Transitional Services into the Authority System;
- (e) greater alignment between delivery and operational organisations;

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (f) clear governance over Transitional Services Requirements; and
- (g) a reduction in the gap between capability and business requirement.

5.2.4 The requirements for transition planning and support are listed below:

Requirement No.	Level	Requirement
	2	Develop Transition Strategy
	3	The Supplier shall support the Authority or its nominated representative in the creation, maintenance and execution of standards, reusable Policies, Procedures and Processes for TS Service Transition and TS Exit.
	2	Create Policies and Procedures
5.2.4.1	3	The Supplier shall work in accordance with the Transition Planning and Support processes as set out in the agreed TS Service Operations Manual.
5.2.4.2	3	The Supplier shall support all transition activities in accordance with the Transition Planning and Support processes as set out in the agreed TS Service Operations Manual.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
5.2.4.3	2	Support to TS Project Request
5.2.4.4	3	The Supplier shall on request from the Authority, support in the early stage development of the services aspects of a Project Proposal in the capture, collation and production of a Project Proposal in support of a TS Project.
	2	Transition Planning
5.2.4.5	3	The Supplier shall support the Authority in the discovery, identification and agreement of Service Requirements to develop a Service Design package.
5.2.4.6	3	The Supplier shall provide details to the Authority of the design for new Transitional Service requirements on request from the Authority.
5.2.4.7	3	The Supplier shall support the Authority in the creation of requested Service Design packages and transition models which shall form the basis for all Service Transition. This shall include, but not be limited to: (i) the review of service requirements, transition plans, and any associated documentation; and (ii) providing resource and delivery time estimates.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
5.2.4.8	3	The Supplier shall obtain appropriate approval from the Authority for all Service Design packages before instigating further transition activities.
5.2.4.9	3	The Supplier shall support the Authority in ensuring that sufficient and appropriate resources are identified and available to deliver Service Design packages to time, quality and cost constraints.
5.2.4.10	3	The Supplier shall support the Authority in ensuring that service risks to failure and disruption across the introduction of new TS services have been fully investigated, understood and mitigating actions are in place with appropriate control and management.
5.2.4.11	3	The Supplier shall ensure the completeness and consistency of all inputs/outputs to transition plans they provide to the Authority.
5.2.4.12	3	The Supplier shall work and collaborate with the Authority in any review as a result of the Supplier's non-compliance with the Transition Planning and Support processes as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Authority.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Manage and coordinate transition
5.2.4.13	3	The Supplier shall support and participate in Service Design activities as coordinated and directed by the Authority.
5.2.4.14	3	The Supplier shall support the Authority in the creation of an Early Life Support plan.
5.2.4.15	3	The Supplier shall support the Authority and coordinate agreed activities to implement the agreed service delivery and support ITSM processes, tools and governance required to support the introduction of changed Transitional Services.
5.2.4.16	3	The Supplier shall ensure that during the course of transition activities the integrity of in situ TS Assets, Transitional Services and components thereof and Configurations Items is maintained.
5.2.4.17	3	The Supplier shall support the Authority in completing the service handover pack and support in making respective contributions available via the Service Knowledge Management System (" SKMS ").
5.2.4.18	3	The Supplier shall support the Authority in managing all TS service transition activities in compliance with Annex 5 (TS Security Management).

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

5.3 TS Change and Evaluation Management

5.3.1 The Supplier shall include the following steps in the TS Change and Evaluation Management lifecycle:

- (a) register requests for TS Change (including TS Service Change or TS Operational Change) ;
- (b) categorise change;
- (c) govern emergency TS Change;
- (d) govern TS Contract Change;
- (e) govern TS Operational Change; and
- (f) review and close TS Change.

5.3.2 The purpose of TS Change and Evaluation Management is to identify, control and account for TS Assets and TS Configuration Items (TS CIs), protecting and ensuring their integrity across the service lifecycle.

5.3.3 The benefit of effective TS Change and Evaluation Management to the Authority is that it:

- (a) prioritises and responds to business driven demand for change to the Transitional Services;
- (b) implements changes that meet the Authority's agreed Service Requirements while optimising efficiency;
- (c) contributes to meeting operational governance, legal, contractual and regulatory requirements;
- (d) reduces failed changes and service disruption, defects and re-work;
- (e) delivers change consistently, promptly within expected timescales;
- (f) contributes to improved estimations of quality, time and cost of change;

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (g) aids in productivity of resources by minimising disruption due to high levels of unplanned or emergency change thus improving the efficiency and effectiveness of service availability;
- (h) provides a single tracking facility for all changes through the service lifecycle and to TS Assets;
- (i) assess the risks associated to the transition of the Transitional Services, both new and existing; and
- (j) increases service quality through appropriate impact assessment of TS Changes, thus preventing Incidents.

5.3.4 The Service Requirements for TS Change and Evaluation Management are listed below:

Requirement No	Level	Requirement
	2	General Requirements
5.3.4.1	3	The Supplier shall support and provide input into the development and maintenance of the Authority's TS Change and Evaluation Management Policies, Processes and Procedures.
5.3.4.2	3	The Supplier shall at all times, work in accordance with the TS Change and Evaluation Management Processes as set out in the agreed TS Service Operations Manual.
5.3.4.3	3	The Supplier shall work and collaborate with the Authority in any review as a result of the Supplier's non-compliance with the TS Change and Evaluation Management processes as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Authority.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No	Level	Requirement
5.3.4.4	3	The Supplier shall provide TS Change and Evaluation Management for the Transitional Services as set out in this Annex 2 Appendix A and the agreed TS Service Operations Manual.
	2	Request For TS Change management
5.3.4.5	3	The Supplier shall raise requests to the Authority for changes including but not limited to: TS Operational Changes (including standard, pre-approved and emergency changes as set out in the agreed TS Service Operations Manual) and TS Contract Changes in accordance with Schedule 22 (<i>Change Control Procedure, Service Requests and Projects</i>).
5.3.4.6	3	The Supplier shall support the Authority in addressing governance concerns in relation to TS Changes raised by the Authority in accordance with Schedule 22 (<i>Change Control Procedure, Service Requests and Projects</i>).

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No	Level	Requirement
5.3.4.7	3	The Supplier shall ensure that all Change Requests they submit contain the information set out in Schedule 22 (<i>Change Control Procedure, Service Requests and Projects</i>) including but not limited to: (i) verified implementation plans; (ii) post implementation review; (iii) acceptance criteria; (iv) back out plans or Remediation Plans; and (v) plans for handover to support.
5.3.4.8	3	The Supplier shall ensure that Approved TS Changes are only implemented by Supplier TS Personnel or authorised representatives in accordance with Schedule 22 (<i>Change Control Procedure, Service Requests and Projects</i>).
5.3.4.9	3	The Supplier shall ensure all TS Contract Changes employ a consistent way of working and are deployed in accordance with Schedule 22 (<i>Change Control Procedure, Service Requests and Projects</i>).
5.3.4.10	3	The Supplier shall maintain and provide the Authority with a list of nominated approved Supplier Personnel who are authorised to request TS Changes.
5.3.4.11	3	The Supplier shall participate in the activities of the Authority's Change Advisory Board (CAB) including but not limited to emergency CAB and the reviews of changes.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No	Level	Requirement
5.3.4.12	3	The Supplier shall support the Authority in identifying and developing TS Contract Changes and TS Operational Changes.
5.3.4.13	3	The Supplier shall provide all information relating to pre-approved TS Operational Changes to the Authority for inclusion in the TS Product and Service Catalogue.
5.3.4.14	3	The Supplier shall inform the Authority of any failure of any pre-approved TS Operational Change.
	2	Review, Monitor, Report and Close
5.3.4.15	3	The Supplier shall ensure that any change to the Transitional Services shall be undertaken in accordance with Schedule 22 (<i>Change Control Procedure, Service Requests and Projects</i>).
5.3.4.16	3	The Supplier shall assess the environmental impact of the introduction of any new Transitional Service, or any architecturally significant change to any existing Transitional Service, in accordance with the Change Control Procedure.
5.3.4.17	3	The Supplier shall support the Authority in analysing and reporting on the management of TS Change in accordance with Schedule 22 (<i>Change Control Procedure, Service Requests and Projects</i>).

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No	Level	Requirement
5.3.4.18	3	The Supplier shall participate and contribute to post implementation reviews.
5.3.4.19	3	The Supplier shall support Other Suppliers via the Authority to ensure that all activities/tasks for a given TS Change have the appropriate ownership.

5.4 TS Knowledge Management

- 5.4.1 TS Knowledge Management is the provision of, and access to, an appropriate store of knowledge and information artefacts relating to the provision, support and maintenance of Transitional Services. It enables the provision of quality Transitional Services and contribute to the provision of quality End to End Services by ensuring that those responsible for managing the Transitional Services and End to End Services are able to do so with access to all current, relevant and appropriate information.
- 5.4.2 The purpose of TS Knowledge Management is to ensure that the right person has the right knowledge at the right time to deliver and support the Transitional Services provided to the Authority.
- 5.4.3 TS Knowledge Management is a key service element. Effective TS Knowledge Management is a powerful asset for people in all roles across all stages of the Service Delivery lifecycle. It should be the primary method for support individuals and teams to share data, information and knowledge about all facets of service. TS Knowledge Management needs to include, but is not limited to:
- (a) user profiling and demand characteristics;
 - (b) Service Desk scripting and system for TS Knowledge Management; and

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

(c) known errors.

5.4.4 The Service Requirements for TS Knowledge Management are listed below:

Requirement No.	Level	Requirement
	2	General Requirements
5.4.4.1	3	The Supplier shall at all times, work in accordance with the TS Knowledge Management processes as set out in the agreed TS Service Operations Manual.
5.4.4.2	3	The Supplier shall work and collaborate with the Authority in any review required as a result of the Supplier's non-compliance with the TS Knowledge Management processes as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Authority.
5.4.4.3	3	The Supplier shall provide TS Knowledge Management for the Transitional Services as set out in this Annex 2 Appendix A and the agreed TS Service Operations Manual.
	2	Service Knowledge Management System
5.4.4.4	3	The Supplier shall use the Service Knowledge Management System (SKMS) provided by the Authority.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
5.4.4.5	3	The Supplier shall support the Authority in the production, maintenance and assurance of up-to-date information for inclusion in the SKMS, to include but not limited to : (i) methods to resolve Incidents; (ii) known errors; (iii) Service Desk scripts; (iv) self help articles; and (v) frequently asked questions (FAQs).
	2	Monitor and Report
5.4.4.6	3	The Supplier shall work and collaborate with the Authority to carry out conformance reviews and audits to ensure the integrity and accuracy of data in the SKMS.
5.4.4.7	3	When Supplier related data is found in the SKMS that is inaccurate, incomplete or lacks integrity, the Supplier shall support the Authority in correcting or removing such data.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Knowledge Management communication
5.4.4.8	3	The Supplier shall inform the Authority of any new changes to the data within the SKMS in accordance with the TS Knowledge Management processes as set out in the agreed TS Service Operations Manual.
	2	Skills, Knowledge and Education
5.4.4.9	3	The Supplier shall ensure that Supplier Personnel required to visit a prison site to deliver the Transitional Services have completed the Prison Site Visit Awareness Training before they visit the prison to ensure the safety of the Supplier Personnel and the prison facilities being visited.
5.4.4.10	3	Where required, the Supplier shall attend the training sessions on utilisation of the SKMS organised by the Authority.
5.4.4.11	3	The Supplier shall ensure that the Supplier's personnel that visit Authority Sites are familiar with the Authority Site access requirements for individual sites.

5.5 TS Release and Deployment Management

- 5.5.1 The Supplier shall provide TS Release and Deployment Management to support the following steps in the TS Release and Deployment Management lifecycle:

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (a) review and update the Release Policy;
- (b) accept Service Design packages;
- (c) build, test and deployment preparations;
- (d) build and test;
- (e) coordinate and manage operational acceptance testing, Service Management, acceptance testing User Acceptance Testing and pilot testing;
- (f) plan and prepare for deployment;
- (g) transfer, deploy and retire and decommission;
- (h) provide early life support;
- (i) verify service deployment; and
- (j) review and close deployment.

5.5.2 The purpose for the TS Release and Deployment Management process is to assemble and position all elements of services into all controlled Authority IT environments and establish effective use of new or changed Transitional Services, covering the full scope of the TS Assets and TS Configuration Items.

5.5.3 The benefit of an effective and efficient TS Release and Deployment Management process is that it adds a consistent and effective means to deliver change in to all IT controlled environments, minimising risk and cost. It also provides assurance to the Authority that new or changed Transitional Services deployed on to the estate derive their full business benefit by establishing an auditable process for tracing requirements from development through to delivery.

5.5.4 The Service Requirements for TS Release and Deployment Management are listed below:

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	General Requirements
5.5.4.1	3	The Supplier shall at all times, work in accordance with the TS Release and Deployment Management processes as set out in the agreed TS Service Operations Manual.
5.5.4.2	3	The Supplier shall support the Authority in maintaining and updating the TS Release Schedule and any associated release plan(s) as per the TS Release and Deployment Management processes as set out in the agreed TS Service Operations Manual.
5.5.4.3	3	The Supplier shall provide Release Documentation to the Authority, including but not limited to: (i) release Plans; (ii) release Packages; and (iii) implementation activities.
5.5.4.4	3	The Supplier shall produce and submit to the Authority impact analysis and potential mitigating actions in support of the TS Release and Deployment Management planning process.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
5.5.4.5	3	The Supplier shall ensure that all TS Assets and TS Configuration Items included in a release package are updated in the Configuration Management System (CMS) and in all relevant documentation as part of the execution of the Release in accordance with the TS Release and Deployment Management processes as set out in the agreed TS Service Operations Manual.
5.5.4.6	3	The Supplier shall work and collaborate with the Authority in any review required as a result of the Supplier's non-compliance with the TS Release and Deployment Management processes as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Authority.
5.5.4.7	3	The Supplier shall provide TS Release and Deployment Management for the Transitional Services in accordance with the agreed TS Service Operations Manual.

5.6 TS Service Asset and Configuration Management

- 5.6.1 The purpose of TS Service Asset and Configuration Management (" **TS SACM**") is to identify and control Service Assets and TS Configuration Items (CIs) by recording and reporting the status of TS Assets and TS CIs and by governing the performance of periodic audits to verify the accuracy and completeness of data held within appropriate repositories.
- 5.6.2 Optimising the performance of TS Assets and configurations improves the overall service performance and optimises the costs and minimises risks caused by poorly managed TS Assets, e.g. service outages, incorrect licence fees and failed audits.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

5.6.3 Effective TS SACM can significantly improve the overall service performance by enabling the Supplier to:

- (a) reduce the instances of quality and compliance issues;
- (b) manage the compliance to policies, standards, legal and regulatory obligations;
- (c) manage service quality and costs;
- (d) gain a better understanding of risk level during and after TS Change;
- (e) optimise the performance of TS Assets and TS CIs thus delivering improved levels of service;
- (f) minimises the disruption and costs associated with poorly managed TS Assets;
- (g) provides accurate information on all Transitional Services and environments deployed and support the TS Change and Evaluation Management Process; and
- (h) scope TS Assets including any resource or capability. The TS Assets of the Supplier include anything that could contribute to the delivery of Transitional Service. TS Assets include but are not limited to:
 - (i) management;
 - (ii) organisation;
 - (iii) process;
 - (iv) knowledge;
 - (v) people;
 - (vi) information;
 - (vii) applications;

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (viii) infrastructure; or
- (ix) financial capital.

5.6.4 The Service Requirements for TS Service Asset and Configuration Management are listed below:

Requirement No.	Level	Requirement
	2	General Requirements
5.6.4.1	3	The Supplier shall ensure that TS Configuration Items relating to the Transitional Services are identified and their relationships recorded and reported to the Authority in accordance with the TS Service Asset Configuration Management processes as set out in the agreed TS Service Operations Manual.
5.6.4.2	3	The Supplier shall perform TS Service Asset and Configuration Management activities in accordance with the TS Service Asset and Configuration Management processes as set out in the agreed TS Service Operations Manual.
5.6.4.3	3	The Supplier shall either: (i) utilise the Authority’s Configuration Management Database (" CMDB "); or (ii) implement a CMDB that supports the Service Asset and Configuration Management processes, within the agreed TS Service Operations Manual and interfaces with the Authority’s CMDB.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
5.6.4.4	3	The Supplier shall identify and record the relationships between TS Configuration Items within their Transitional Service portfolio and shall report the relationships to the Authority in accordance with the TS Service Asset Configuration Management processes as set out in the agreed TS Service Operations Manual.
5.6.4.5	3	The Supplier shall at all times work in accordance with the TS Service Asset and Configuration Management processes as set out in the agreed TS Service Operations Manual.
5.6.4.6	3	The Supplier shall support the identification of TS CIs and TS Assets as required by the Authority and in accordance with the TS Service Asset and Configuration Management processes as set out in the agreed TS Service Operations Manual.
5.6.4.7	3	The Supplier shall provide and maintain a list of Supplier Personnel who require access to the CMDB.
5.6.4.8	3	The Supplier shall work and collaborate with the Authority in any review as a result of the Supplier's non-compliance with the Authority's TS Service Asset and Configuration Management processes and procedures as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Authority.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
5.6.4.9	3	The Supplier shall provide TS Service Asset and Configuration Management for the Transitional Services.
	2	Audit, Monitoring and Reporting
5.6.4.10	3	The Supplier shall support the Authority in providing quality assurance, data reconciliation and audit activities against CI's data held within the CMDB and data held in the Transitional Services CMDBs to ensure compliance with the TS Service Asset and Configuration Management processes as set out in the agreed TS Service Operations Manual.
5.6.4.11	3	The Supplier shall support the Authority to identify and implement remedial actions where it has been identified that the CMDB has breached TS Service Level Thresholds relating to accuracy or currency set out in Annex 3 (<i>TS Performance Levels</i>).
	2	Updates to Configuration Management
5.6.4.12	3	The Supplier shall support the Authority to ensure updates to the CMS are performed in accordance with the TS Service Asset and Configuration Management process as set out in the agreed TS Service Operations Manual and within the TS Service Levels set out in Annex 3 (<i>TS Performance Levels</i>).

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
5.6.4.13	3	The Supplier shall support the Authority in ensuring that updates to the CMS are automatically synchronised unless otherwise agreed with the Authority.
5.6.4.14	3	The Supplier shall either interface with or make use of the Definitive Media Library (DML) provided by the Authority.
5.6.4.15	3	The Supplier shall ensure that only TS Software contained in the DML is deployed to the Authority's estate.
5.6.4.16	3	The Supplier shall support the Authority in the implementation of the Authority's asset management policy.
	2	TS Asset Management
5.6.4.17	3	The Supplier shall ensure that TS Assets relating to the Transitional Services are identified and reported to the Authority in accordance with the TS SACM processes as set out in the agreed TS Service Operations Manual.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
5.6.4.18	3	The Supplier shall either: (i) utilise the Authority's Asset management system; or (ii) implement an asset management system that supports the TS Service Asset and Configuration Management process and TS Asset and interfaces with the Authority's asset management system.
5.6.4.19	3	The Supplier shall maintain accurate records of TS Assets used to deliver the Transitional Services. This includes Exclusive Assets, New TS Assets (that have been purchased by the Supplier), Non-Exclusive Assets and is irrespective of the ownership of each TS Asset. Where the Supplier and Other Suppliers use Non-Exclusive Assets then a reference should be made in the attributes to that TS Asset.
5.6.4.20	3	The Supplier shall ensure that they record all agreed attributes of a TS Asset so that it can be uniquely defined in accordance with the SACM processes as set out in the agreed TS Service Operations Manual.
	2	Disposal of TS Assets
5.6.4.21	3	The Supplier shall support the Authority when requested to ensure that hardware is appropriately wiped against approved standards (in accordance with the Authority's asset disposal policies) in readiness for disposal or redeployment across the Authority's estate.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

5.7 TS Service Validation and Testing

- 5.7.1 The Authority places a strong emphasis on the quality and value of testing performed by suppliers and ensuring their testing activities integrate into the testing lifecycle. The Authority has defined an overarching Test Strategy covering the whole lifecycle, with which the Supplier must comply. The Authority Test Strategy sets out a number of key principles to ensure that testing representatives are engaged early in the lifecycle, have sufficient independence and operate in a repeatable and measurable manner to well defined products, processes and controls.
- 5.7.2 The Supplier is required to create a Project Test Strategy setting out their approach to testing for the scope of the Transitional Services they provide to the Authority.
- 5.7.3 The Authority may assure the Supplier's testing processes, throughout the testing lifecycle.
- 5.7.4 The Service Requirements for TS Service Validation and Testing are listed below:

Requirement No.	Level	Requirement
	2	Testing Policies and Procedures
5.7.4.1	3	All testing conducted by the Supplier shall be completed in accordance with Schedule 14 (<i>Testing Procedures</i>).

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
5.7.4.2	3	The Supplier shall support the Authority and Other Suppliers in the creation of each TS Project Test Strategy and/or Test Plan as required, setting out the testing activities for a new Transitional Service or change to an existing Transitional Service as applicable.
5.7.4.3	3	The Supplier shall, when required by the Authority, produce a TS Project Test Strategy and/or Test Plan and submit to the Authority for Approval in accordance with Schedule 13 (<i>Implementation</i>).
5.7.4.4	3	The Supplier shall appoint a suitably qualified Test Manager where the Supplier has responsibilities for conducting or supporting testing in relation to a project or change. The Supplier Test Manager shall be responsible for all testing performed or supported by the Supplier who shall be the Single Point of Contact for the Authority for all such Supplier testing activities.
5.7.4.5	3	The Supplier shall not pass a Test item out of a Test phase until the associated Test Success Criteria have been met in accordance with Schedule 14 (<i>Testing Procedures</i>) unless otherwise agreed with the Authority. If a failure to satisfy Test Success Criteria results or is likely to result in a failure by the Supplier to meet a TS Milestone, the Supplier shall create a Rectification Plan in accordance with Schedule 14 and Clause 25.1 and submit to the Authority for Approval.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
5.7.4.6	3	The Supplier shall support Test assurance and test witnessing activities conducted by or on behalf of the Authority. Such assurance activities do not diminish the Supplier's obligations to achieve the applicable Test Success Criteria and TS Service Levels.
	2	TS Test Environment Provisioning & Management
5.7.4.7	3	The Supplier shall ensure all Test environments, for the Transitional Services they provide, have the ability to be partly or fully disconnected from the Master Time Reference to allow different types of testing to be performed e.g. to roll forwards and backwards in time.
5.7.4.8	3	The Supplier shall ensure that Test environments are treated as TS Assets that are managed in accordance with the SACM processes as set out in the agreed TS Service Operations Manual.
5.7.4.9	3	The Supplier shall submit requests to the Authority for the establishment, use and decommissioning of Test environments in line with the TS Project Test Strategy/Plan.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
5.7.4.10	3	The Supplier shall make available to any requesting Other Supplier, the Test environments provisioned via the Authority as set out in the TS Project Test Strategy.
	2	Unit/Component Testing
5.7.4.11	3	The Supplier shall be fully accountable for the planning, design, implementation, execution and reporting for unit/component Testing for all new and/or modified components it is providing in relation to a project or change, as specified in the associated TS Project Test Strategy Approved by the Authority.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	System Testing
5.7.4.12	3	The Supplier shall be accountable for the planning, design, implementation, execution and reporting for System Testing for all new and/or modified components it is providing in relation to a TS Project or TS Change to be undertaken in accordance with Schedule 14 (<i>Testing Procedure</i>).
5.7.4.13	3	The Supplier shall support System Testing planning, design, implementation, execution and reporting conducted by Other Suppliers as identified in the associated TS Project Test Strategy Approved by the Authority.
	2	Systems Integration Testing
5.7.4.14	3	The Supplier shall support the Authority in the planning, design, implementation, execution and reporting of System Integration Testing.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Operational Acceptance Testing
5.7.4.15	3	The Supplier shall support the Authority in the planning, design, implementation, execution and reporting of operational acceptance testing.
	2	User Acceptance Testing
5.7.4.16	3	The Supplier shall support the Authority in the planning, design, implementation, execution and reporting of User Acceptance Testing.
	2	Service Management Acceptance Testing
5.7.4.17	3	The Supplier shall support the Authority in the planning, design, implementation, execution and reporting of Service Management acceptance testing.
	2	Pilot Testing
5.7.4.18	3	The Supplier shall support the Authority in the planning, design, implementation, execution and reporting of pilot testing.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Break/Fix Testing
5.7.4.19	3	The Supplier shall be fully accountable for the planning, design, implementation, execution and reporting of break/fix testing of the components for which it is responsible.
5.7.4.20	3	The Supplier shall support the Authority and Other Suppliers in the planning, design, implementation, execution and reporting of Break/Fix Testing.
5.7.4.21	2	Maintenance Release Testing
5.7.4.22	3	The Supplier shall be fully accountable for the planning, design, implementation, execution and reporting of maintenance release testing of the components for which it is responsible.
5.7.4.23	3	The Supplier shall support Other Suppliers in the planning, design, implementation, execution and reporting of maintenance release testing.
5.7.4.24	2	Transfer of Test Assets for Live Service
5.7.4.25	3	The Supplier shall ensure that all test TS Assets it has created or modified are managed in accordance with the TS SACM Processes as set out in the agreed TS Service Operations Manual.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

6 TS SERVICE OPERATION

6.1 Introduction

6.1.1 The purpose of TS Service Operation is the coordination and delivery of the activities, processes and functions required to deliver and manage the Transitional Services to agreed quality and Transitional Services to the Authority. TS Service Operation covers the responsibilities for the ongoing management of the technology used to deliver and support the Transitional Services.

6.2 TS Access Management

6.2.1 TS Access Management is the process of granting authorised End Users the right to use the Transitional Services and helps to protect the confidentiality, integrity and availability of TS Assets and information.

6.2.2 A controlled and managed TS Access Management process delivers benefit to the Authority by:

- (a) ensuring that the organization is able to maintain the confidentiality of its information more effectively;
- (b) employees having the right level of access to execute their jobs effectively;
- (c) the ability to audit use of services and to trace the abuse of services; and
- (d) the ability to easily revoke access rights when needed.

6.2.3 The Service Requirements for TS Access Management are listed below:

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	General Requirements
6.2.3.1	3	The Supplier shall work in accordance with the TS Access Management processes and the Supplier Personnel Access Management processes as set out in the agreed TS Service Operations Manual, when the Supplier's Personnel requires access to the Authority Sites, Other Supplier's Sites or Other Supplier's ICT environment.
6.2.3.2	3	The Supplier shall work and collaborate with the Authority in any review required as a result of the Supplier's non-compliance with the Authority's TS Access Management policy and the TS Access Management processes as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed with the Authority.
6.2.3.3	3	The Supplier shall work and collaborate with the Authority in any review required as a result of the Supplier's non-compliance with the Supplier Personnel Access Management processes as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Authority.

6.3 TS Event Management

- 6.3.1 The TS Event Management process shall detect Events, analyse and then determine the appropriate control activity or action to prevent an Incident and/or service interruption.
- 6.3.2 Events need to be identified and set up such that their occurrence enables the communication of operational information.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 6.3.3 The benefit of effective TS Event Management to the Authority is that it:
- (a) provides mechanisms for early detection of incidents. In many cases, it is possible for the incident to be detected and assigned to the appropriate group for action before any actual service outage occurs;
 - (b) can signal, when integrated into other TS Service Management processes, status changes or exceptions that allow the appropriate person or team to respond promptly, thus improving the performance of the process; and
 - (c) provides a basis for automated operations, thus increasing efficiencies and allowing expensive human resources to be used for more innovative work.

6.3.4 The Service Requirements for TS Event Management are listed below:

Requirement No.	Level	Requirement
	2	General Requirements
6.3.4.1	3	The Supplier shall at all times, work in accordance comply with the TS Event Management Processes as set out in the agreed TS Service Operations Manual.
6.3.4.2	3	The Supplier shall provide Event monitoring information to the Authority in accordance with the TS Event Management Processes as set out in the agreed TS Service Operations Manual.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
6.3.4.3	3	The Supplier shall work and collaborate with the Authority in any review required as a result of the Supplier's non-compliance with the TS Event Management processes as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Authority.
6.3.4.4	3	The Supplier shall provide TS Event Management for the Transitional Services as set out in this Annex 2 Appendix A and the agreed TS Service Operations Manual.
	2	Support Alert Management
6.3.4.5		The Supplier shall propose defined Event thresholds for the Transitional Services to the Authority for approval.
6.3.4.6	3	The Supplier shall support the Authority in the investigation and resolution of Events that have exceeded a pre-defined threshold.

6.4 TS Incident Management

6.4.1 The Authority requires TS Incident Management to be the process that handles all failures, faults or questions reported by End Users via the Service Desk or which are automatically detected and reported by TS Event Management. TS Incident Management should include the use of Incident Models that include the following steps within the TS Incident Management lifecycle:

- (a) log and categorisation of the TS Incident;

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) diagnosis and the steps required to handle the TS Incident;
 - (c) assign responsibilities for the performance and execution of first-level, second-level and third-level support, analysis, diagnosis and resolution of the incident;
 - (d) set expectations on timescales and thresholds for the completion of identified actions;
 - (e) manage the escalation activities based on pre-defined hierarchy and communication plan;
 - (f) identify measures, when appropriate, to minimise future disruptions; and
 - (g) manage the end-to-end Incident lifecycle.
- 6.4.2 The purpose of TS Incident Management is to restore the Transitional Services as quickly as possible and minimise adverse impact and disruption on normal business operations.
- 6.4.3 Effective TS Incident Management allows the business to continue to realise the benefits of enabling ICT technologies and services by:
- (a) minimising downtime of the Transitional Services, and where applicable the End to End Services, to the Authority's business;
 - (b) ensuring the Transitional Services are aligned with day-to-day business priorities;
 - (c) identifying potential service improvements; and
 - (d) identifying additional service or training requirements.
- 6.4.4 The Service Requirements for TS Incident Management are listed below:

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	General Requirements
6.4.4.1	3	The Supplier shall support the Authority in developing, documenting, implementing and maintaining TS Incident Management processes as set out in the agreed TS Service Operations Manual.
6.4.4.2	3	The Supplier shall at all times, work in accordance with the TS Incident Management processes as set out in the agreed TS Service Operations Manual.
6.4.4.3	3	The Supplier shall proactively support the Authority to deliver the required TS Service Levels, for TS Service Incident management and TS Security Incident management as set out in Annex 3 (<i>TS Performance Levels</i>).
6.4.4.4	3	The Supplier shall ensure that Security Incidents and security-related Events are categorised by Severity / Priority level as defined in Annex 3 (<i>TS Performance Levels</i>)
6.4.4.5	3	The Supplier shall work and collaborate with the Authority in any review required as a result of the Other Suppliers non-compliance with the Incident Management processes as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Authority.
6.4.4.6	3	The Supplier shall utilise the Authority's Incident Management System.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
6.4.4.7	3	The Supplier shall ensure that the TS Incident Management process within their own organisation provides an audit trail that complies with the Incident Management processes as set out in the agreed TS Service Operations Manual relating to the management and resolution of TS Incidents.
6.4.4.8	3	The Supplier shall adopt and implement the TS Incident Severity Levels and Definitions and TS Incident Resolution Priorities set out in Annex 3 (<i>TS Performance Levels</i>).
6.4.4.9	3	The Supplier shall monitor and manage allocated TS Incidents for which they are responsible in accordance with the TS Incident Management processes as set out in the agreed TS Service Operations Manual and with the TS Service Levels set out in Annex 3 (<i>TS Performance Levels</i>).
6.4.4.10	3	The Supplier shall update the TS Incident record with all relevant information relating to the TS Incident in accordance with the TS Incident Management processes as set out in the agreed TS Service Operations Manual.
6.4.4.11	3	The Supplier shall adhere to the TS Incident Severity Level Definitions and TS Incident Resolution Priorities as specified by the Authority in Annex 3 (<i>TS Performance Levels</i>).

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
6.4.4.12	3	The Supplier shall support the Authority in the continual improvement of the TS Incident Management processes via the identification and implementation of means by which the volume of TS Incidents are reduced over the TS Term.
6.4.4.13	3	The Supplier shall provide TS Incident Management for the Transitional Services as set out in this Annex 2 Appendix A and the agreed TS Service Operations Manual.
	2	Provide TS Incident Management Support
6.4.4.14	3	The Supplier shall provide appropriately skilled resources to fulfil their obligations as set out in the TS Incident Management processes as set out in the agreed TS Service Operations Manual.
6.4.4.15	3	The Supplier shall support the Authority to restore normal the Transitional Services or provide a Workaround agreed by the Authority during the resolution of TS Incidents.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Monitoring and Reporting of TS Incident Management
6.4.4.16	3	The Supplier shall provide progress notifications to the Authority on all current TS Incidents including progress notifications where the frequency of such notifications is in accordance with the Authority TS Incident Management processes as set out in the agreed TS Service Operations Manual and the TS Service Levels as set out in Annex 3 (<i>TS Performance Levels</i>).
6.4.4.17	3	The Supplier shall make changes to the assigned Incident Resolution Priority of a TS Incident when directed to do so by the Authority.
	2	TS Incident Communications
6.4.4.18	3	The Supplier shall proactively notify the Authority of any TS Incident relating to the Transitional Service that is known to be in breach or highly likely to breach the TS Service Levels as defined in Annex 3 (<i>TS Performance Levels</i>) via the Service Desk.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Support TS Incident Management
6.4.4.19	3	The Supplier shall accept and acknowledge that the Authority shall be the single point of contact with the Authority for the formal progression of all TS Incidents unless otherwise set out in the TS Incident Management processes as set out in the agreed TS Service Operations Manual.
6.4.4.20	3	The Supplier shall acknowledge all TS Incidents correctly assigned to them and return TS Incidents to the Authority that have been wrongly assigned in accordance with the TS Incident Management processes as set out in the agreed TS Service Operations Manual.
6.4.4.21	3	The Supplier following receipt of a TS Incident shall, where necessary, schedule and perform resolution activities with the End User in accordance with the TS Incident Management processes as set out in the agreed TS Service Operations Manual.

6.5 TS Problem Management

- 6.5.1 TS Problem Management deals with the underlying causes of incidents. The functionality of problem records should be similar to those needed for TS Incident Records and also allow for multiple incidents matching against problem records. This service shall include the following steps in the TS Problem Management lifecycle:

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (a) detection;
- (b) capture and categorisation;
- (c) investigation and diagnosis; and
- (d) resolution.

6.5.2 The principal objective of TS Problem Management is to prevent TS Problems from occurring by eliminating recurring TS Incidents and to minimise the impact of TS Incidents that cannot be prevented.

6.5.3 Effective TS Problem Management reduces the impacts to the business of reduced service quality in the Transitional Services, allowing the business to continue to realise the benefits of enabling ICT technologies and services by:

- (a) reducing the number of TS Incidents raised across the estate;
- (b) employing Root Cause Analysis to determine cause of TS Problems and to further eliminate potential issues;
- (c) implementing a permanent fix for all identified problem causes; and
- (d) logging and maintaining known errors and Workarounds to prevent a Transitional Service outage.

6.5.4 The Service Requirements for TS Problem Management are listed below:

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	General Requirements
6.5.4.1	3	The Supplier shall at all times, work in accordance with the TS Problem Management processes as set out in the agreed TS Service Operations Manual.
6.5.4.2	3	The Supplier shall utilise the Authority's TS Problem Management System.
6.5.4.3	3	The Supplier shall work and collaborate with the Authority in any review as a result of the Supplier's non-compliance with the TS Problem Management processes as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Authority.
6.5.4.4	3	The Supplier shall provide TS Problem Management for the Transitional Services as set out in this Annex 2 Appendix A and the agreed TS Service Operations Manual.
	2	Monitor and Report
6.5.4.5	3	The Supplier shall monitor and progress, in line with the TS Service Levels set out in Annex 3 (<i>TS Performance Levels</i>) and the TS Problem Management processes as set out in the agreed TS Service Operations Manual, the TS Problems for which they are responsible.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
6.5.4.6	3	The Supplier shall develop, maintain and provide to the Authority, for inclusion in the SKMS, information on Workarounds, known errors and TS Problems related to the Transitional Services.
	2	Managing the TS Problem Management Lifecycle
6.5.4.7	3	The Supplier shall support the Authority in TS Problem analysis as requested by the Authority including, but not limited to, the provision of information relating to TS Problem trends, volumes and TS Problem solutions.
6.5.4.8	3	The Supplier shall attend TS Problem reviews as requested by the Authority and otherwise take steps to address TS Problems in accordance with Problem Management Process and the agreed TS Service Operations Manual.
	2	Support for TS Problem Management
6.5.4.9	3	The Supplier shall provide status updates on TS Problem resolution to the Authority in accordance with the agreed TS Service Operations Manual.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
6.5.4.10	3	The Supplier shall resolve TS Problems that have been assigned to them in accordance with the TS Problem Management processes as set out in the agreed TS Service Operations Manual.

6.6 TS Request Fulfilment

- 6.6.1 TS Request Fulfilment is the process for managing TS Service Requests. These standard and repeatable changes are initiated via an automated catalogue of Transitional Services and follow the steps within the TS Request Fulfilment lifecycle.
- 6.6.2 The benefit of a centralised, efficient and effective TS Request Fulfilment process is:
- (a) a fast and efficient service improves productivity by delivering services when they are required;
 - (b) improvement to the quality services used through the use of centralised procurement and fulfilment;
 - (c) improved process conformance and reduction in unnecessary bureaucracy and administration in submitting requests and delivering services; and
 - (d) greater control over the Transitional Services on offer.
- 6.6.3 The Service Requirements for TS Request Fulfilment are listed below:

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	General Requirements
6.6.3.1	3	The Supplier shall at all times provide end to end management of TS Service Requests and work in accordance with the TS Request Fulfilment processes as set out in the agreed TS Service Operations Manual.
6.6.3.2	3	The Supplier shall action each TS Service Request they receive from the Authority in accordance with Annex 3 (<i>TS Performance Levels</i>).
6.6.3.3	3	The Supplier shall notify the Authority of any potential breach to the TS Service Levels as defined in Annex 3 (TS Performance Levels) relating to TS Service Requests.
6.6.3.4	3	The Supplier shall support the Authority in the identification and resolution of conflicts in the fulfilment of competing TS Service Requests.
6.6.3.5	3	The Supplier shall work and collaborate with the Authority in any review required as a result of the Supplier's non-compliance with the TS Request Fulfilment processes as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Customer.
6.6.3.6	3	The Supplier shall provide TS Request Fulfilment for the Transitional Services as set out in this Annex 2 Appendix A and the agreed TS Service Operations Manual.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Monitoring and Reporting
6.6.3.7	3	The Supplier shall support the Authority in analysing and reporting on TS Request Fulfilment as set out in the agreed TS Service Operations Manual as requested by the Authority.

6.7 Service Desk

- 6.7.1 The Service Desk function shall provide a single point of contact for the Transitional Services provided to the Authority. It shall consist of appropriately skilled staff responsible for dealing with a variety of service events and should be able to:
- (a) leverage expert resource from the Other Suppliers;
 - (b) handle all Incidents and Service Requests; and
 - (c) utilise specialist tools to manage all Events.
- 6.7.2 The Supplier shall provide a support and resolver service for all the Transitional Services.
- 6.7.3 The primary aim of the Service Desk shall be to restore normal service to the End Users as quickly as possible.
- 6.7.4 The primary aims of the Supplier’s support and resolver services shall be:
- (a) to ensure the availability and successful operation of the Transitional Services;
 - (b) to restore normal service to the End Users as quickly as possible.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

6.7.5 The Service Requirements for supporting the Service Desk are listed below:

Requirement No.	Level	Requirement
	2	General Requirements
6.7.5.1	3	The Supplier shall at all times work in accordance with the Service Desk policies, processes and procedures as set out in the agreed TS Service Operations Manual and provide the required Transitional Service support for the Transitional Service or Service Components to fulfil the TS Service Levels defined in Annex 3 (TS Performance Levels).
6.7.5.2	3	The Supplier shall provide English speaking resources to support the Service Desk in the provision of ITIL processes.
6.7.5.3	3	The Supplier shall provide updates and information and interface with the Incident processes as set out in the agreed TS Service Operations Manual.
6.7.5.4	3	The Supplier shall support the Authority in the provision of a Service Desk function in accordance with the Service Desk Processes as set out in the agreed TS Service Operations Manual.
6.7.5.5	3	The Supplier shall provide the Authority with all appropriate information on Incidents, Problems, known errors, agreed Workarounds, Supplier's Releases and their inter-relationships in support of the Transitional Services.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Skills, Knowledge and Education
6.7.5.6	3	The Supplier shall ensure that personnel who interact with the Service Desk are appropriately trained and are capable of working to the Incident Management, Problem Management, TS Service Request and Knowledge Management processes as set out in this Appendix A to Annex 2 (<i>TS Services Description</i>), Annex 3 (<i>TS Performance Levels</i>) and the agreed TS Service Operations Manual.
6.7.5.7	3	The Supplier shall ensure that personnel who interact with the Service Desk have access to the Service Knowledge Management System or shall support the Authority to ensure that the personnel of the Supplier be granted access to the Authority's SKMS.
6.7.5.8	3	The Supplier shall participate in the collation, provision and dissemination of skills and knowledge required in providing support for the Transitional Services.
	2	Communication
6.7.5.9	3	The Supplier shall ensure that all first contact communication with End Users is managed and coordinated via the Authority's Service Desk.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
6.7.5.10	3	The Supplier shall ensure that all subsequent (after first contact) communication with End Users is recorded in the Incident record and is made available to the Service Desk in accordance with the Service Desk processes as set out in the agreed TS Service Operations Manual.

6.8 TS Technical Management

- 6.8.1 The purpose of TS Technical Management is to perform the proactive and reactive maintenance activities required to keep the Transitional Services, and where applicable the End to End Services, in a fully functional state to minimise adverse impact and disruption on normal business operations.
- 6.8.2 Effective TS Technical Management allows the business to continue to realise the benefits of enabling ICT technologies and services by:
- (a) minimising downtime of the Transitional Services, and where applicable the End to End Services, to the business;
 - (b) ensuring Transitional Services are aligned with day-to-day business priorities; and
 - (c) maintaining alignment between Transitional Services and technology roadmaps.
- 6.8.3 The Supplier shall design, manage, implement and support the technical components that comprise the Transitional Services, including:
- (a) WAN Services; and
 - (b) technical integration of all the Services and interfacing and integration with the End to End Transitional Services.
- 6.8.4 The Service Requirements for TS Technical Management are listed below:

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	WAN Management
6.8.4.1	3	The Supplier shall pro-actively monitor the Transitional Services to address actual or potential changes in performance characteristics to ensure that TS Service Levels as described in Annex 3 (<i>TS Performance Levels</i>) can continue be met by the Supplier.
6.8.4.2	3	The Supplier shall ensure that all TS Software used in the delivery of the Transitional Services shall remain in service life support by the manufacturer unless otherwise agreed by the Authority.
	2	System Software Maintenance and Support
6.8.4.3	3	The Supplier shall provide an evaluation report on the impact of any new version of any TS Software product on the Transitional Services or Authority System where required.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
6.8.4.4	3	Where support for a TS Software product is to be withdrawn, the Supplier shall ensure that a review commences sufficiently early to ensure that: (a) a replacement Product is identified, tested and made available through the TS Product and Service Catalogue; and (b) Changes to the relevant service description(s) are updated in the TS Product and Service Catalogue to reflect the change before the vendor withdraws support for the original Product; and [REDACTED]
6.8.4.5	3	The Supplier shall ensure that all TS Software, unless otherwise agreed by the Authority is supported by the Software vendor or [REDACTED]
6.8.4.6	3	The Supplier shall ensure that all vendor recommended service packs and releases to TS Software are tested in accordance with Schedule14 (<i>Testing Procedures</i>), and scheduled for release in accordance with the TS Release and Deployment Management and TS Change and Evaluation Management processes as set out in the agreed TS Service Operations Manual.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

7 TS CONTINUAL SERVICE IMPROVEMENT

7.1 Introduction

7.1.1 The purpose of TS Continual Service Improvement ("**TS CSI**") is to create and maintain value in the design, introduction, operation and use of the Transitional Services. Through the process of 'Plan, Do, Check and Act' Service Improvement Plans are created based on shortfalls or opportunities identified.

7.2 Identify and Deliver Service Improvement

7.2.1 This service shall include the following steps in the TS Continual Service Improvement lifecycle:

- (a) reviewing management information and trends to ensure that the output of the enabling ITSM processes are achieving the desired results;
- (b) periodically conducting maturity assessments against the process activities and roles associated with the process activities to demonstrate areas of improvement or, conversely, areas of concern;
- (c) periodically conducting audits verifying process compliance;
- (d) reviewing the Transitional Services for improvements;
- (e) making recommendations for approval; and
- (f) conducting periodic customer satisfaction surveys.

7.2.2 The primary purpose of CSI is to continually align and realign the Transitional Services to the changing needs of the Authority by identifying and implementing improvements to the Transitional Services that support the Authority's core business. Improvement activities shall support the lifecycle approach through TS Service Strategy, TS Service Design, and TS Service Operations (each as set out in this Annex 2 Appendix A).

7.2.3 The benefit of 'Identify and Deliver Service Improvement' is that it:

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (a) leads to a continual improvement in Transitional Service quality;
- (b) ensures that the Transitional Services remain continuously aligned to business requirements;
- (c) delivers improvements in cost effectiveness through identifying and implementing reduction in costs and or the capability to improve productivity; and
- (d) identifies opportunities for improvement in all lifecycle stages and processes through monitoring and reporting.

7.2.4 The Service Requirements for Identify and Deliver Service Improvement are listed below:

Requirement No.	Level	Requirement
	2	General Requirements
7.2.4.1	3	The Supplier shall ensure that TS Continual Service Improvement at all times effectively interfaces with all other processes across the TS Service Delivery lifecycle.
	2	Manage and Coordinate
7.2.4.2	3	The Supplier shall support the Authority in identifying and delivering TS Continual Service Improvement to the way Transitional Services are delivered to the Authority.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	TS Continual Service Improvement Programme
7.2.4.3	3	The Supplier shall support the Authority in the production, maintenance, and provision of Service Improvement Plans for those elements of the Transitional Services for which they are responsible and have been identified as being the subject of improvements.
7.2.4.4	3	The Supplier shall engage and contribute in the establishment and delivery of the TS Continual Service Improvement Programme.
7.2.4.5	3	The Supplier shall ensure that they effectively discharge their obligations set out in the relevant Service Improvement Plan to ensure that such Service Improvement Plans are implemented effectively in accordance with the TS Continual Service Improvement Programme.
	2	Support for TS Service Improvement Programme
7.2.4.6	3	The Supplier shall keep the Authority informed of the progress against those Service Improvement Plans where the Supplier is responsible, in whole or part, for the delivery of those Service Improvement Plans.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

7.3 TS Service Measurement and Performance Management

7.3.1 The TS Service Measurement and Performance Management process shall monitor the performance of the management of the Transitional Services. The TS Service Measurement and Performance Management process defines appropriate measures, collects and collates data and provides analytical reports that support the identification and delivery of service improvements. The TS Service Measurement and Performance Management process is set against organisational objectives and targets, as opposed to TS Service Level Management that is centred on contractual obligations and the monitoring and measurement against TS Service Levels.

7.3.2 The benefit of an effective TS Service Measurement and Performance Management process is that it:

- (a) aids and assists the decision making process for ICT Strategy attainment;
- (b) provides information on the performance, availability, capacity and reliability of the Transitional Services;
- (c) provides information on the performance of the Transitional Services;
- (d) helps to identify the areas for service and process improvement;
- (e) provides the means to assess the effectiveness of service and process improvements; and
- (f) provides benchmark and baseline performance data that enable benchmarking activities.

7.3.3 The Service Requirements for TS Service Measurement and Performance Management are listed below:

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	General Requirements
7.3.3.1	3	The Supplier shall support the Authority to develop a strategy for TS Service Measurement and Performance Management.
7.3.3.2	3	The Supplier shall support the Authority to maintain the processes and procedures for TS Service Measurement and Performance Management as set out in the agreed TS Service Operations Manual.
7.3.3.3	3	The Supplier shall at all times work in accordance with the TS Service Measurement and Performance Management processes as set out in the agreed TS Service Operations Manual.
7.3.3.4	3	The Supplier shall support the Authority in identifying any improvements to TS Service Measurement and Performance Management in accordance with the TS Continual Service Improvement Service.
7.3.3.5	3	The Supplier shall work and collaborate with the Authority in any review required as a result of the Supplier's non-compliance with the TS Service Measurement and Performance Management processes as set out in the agreed TS Service Operations Manual and implement any required corrective action that has been agreed by the Authority.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Performance Monitoring
7.3.3.6	3	The Supplier shall support the TS Service Measurement and Performance Management processes and ensure that there are effective interfaces with all the Transitional Services.
7.3.3.7	3	The Supplier shall support the Authority in providing TS Service Measurement and Performance Management processes that use a reporting process that contains measurements that are 'SMART (Specific, Measurable, Attainable, Realistic and Time-bound)'.
7.3.3.8	3	The Supplier shall support the Authority in providing a performance monitoring framework capable of providing different perspectives supporting, but is not limited to: (i) the use of a Performance Scorecard approach showing a mixture of quantitative and qualitative measures; (ii) the differing requirements of the Authority's VIP Sites; (iii) viewable data by the Authority's business unit and/or service consumed by business unit and/or Authority Site; and (iv) sufficient granularity to identify the effects of poor performance and implemented service improvements.
7.3.3.9	3	The Supplier shall be responsible for creating and maintaining the measurement criteria for those TS Service Levels they are responsible for delivering against and as set out in the agreed TS Service Operations Manual.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
7.3.3.10	3	The Supplier shall support the Authority in providing performance information that: (i) enables evaluation of performance of Transitional Services against stated TS Service Levels and Authority objectives and other agreed performance measures; and (ii) enables comparison analysis of service performance against past, present and forecast of future predictions.
	2	Manage Performance Information Quality
7.3.3.11	3	The Supplier shall provide performance information to the Authority as set out in the agreed TS Service Operations Manual.

8 TS SERVICE LIFECYCLE MANAGEMENT

8.1 Introduction

8.1.1 The purpose of TS Service Lifecycle Management is to provide the tools and mechanisms to coordinate and control the Transitional Services and processes, from end to end, to manage the full lifecycle of the Transitional Services.

8.2 IT Service Management Toolset

8.2.1 The requirement for the ITSM Toolset is to ensure that there is a single source of authoritative information on any given service event and that the management of these events, to a successful conclusion, is available, visible, reportable and auditable from one source. The requirements

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

listed below set out the obligations and relationship between the Supplier, the Authority and Other Suppliers in the selection, provision and operation of an end to end ITSM Toolset solution.

- 8.2.2 The ITSM Toolset shall provide a common interface for the management and support to all Transitional Services and ensure that all Other Suppliers, and the Authority have access to clear, accurate, timely and unambiguous information on the state, performance and operation of the Transitional Services provided to the Authority.
- 8.2.3 Access to the management of information is a core requirement in any process management role and having an integrated ITSM Toolset in support of the Service Delivery Lifecycle ("**SDLC**") shall ensure that the Supplier and the Authority can access the timely, informed and accurate information to enable the right discussions to be taken for the right reasons in a timely and effective manner.
- 8.2.4 The Service Requirements for ITSM Toolset are listed below:

Requirement No.	Level	Requirement
	2	General Requirements
8.2.4.1	3	The Supplier shall at all times, work in accordance with the ITSM Toolset processes as set out in the agreed TS Service Operations Manual.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
8.2.4.2	3	The Supplier shall utilise the ITSM Toolset provided by the Authority for the management of service events across the SDLC. The use of the ITSM Toolset is required to ensure the delivery of the following processes: (i) TS Event Management; (ii) TS Incident Management; (iii) TS Problem Management; (iv) TS Change and Evaluation Management; (v) TS Knowledge Management; (vi) TS Product and Service Catalogue Management; (vii) TS Service Asset and Configuration Management; and (viii) TS Continual Service Improvement;
8.2.4.3	3	The Supplier shall ensure all relevant TS Supplier Personnel are suitably skilled to utilise the ITSM Toolset, including in accordance with the ITSM Toolset processes as set out in the agreed TS Service Operations Manual.

8.3 TS Architecture Management

8.3.1 This includes the following areas of TS Enterprise Architecture Management, TS Solution Architecture Management and TS Deployed Architecture Management to provide:

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (a) vision & Strategy definition;
 - (b) architecture rules management (creation and maintenance of architecture and technology principles, policies, standards and reference models);
 - (c) architecture specification (business, information systems & information technology);
 - (d) improvement planning (opportunities, solutions, migration & transformation);
 - (e) realisation (including acquisition and implementation governance);
 - (f) architecture governance (architecture change management & requirements management); and
 - (g) architecture compliance and alignment monitoring.
- 8.3.2 The purpose of TS Enterprise Architecture Management is to support the translation of the Authority's business vision and strategies into effective enterprise change; and to ensure the continuing alignment of IS/IT services provision to the Authority's business objectives.
- 8.3.3 The purpose of TS Solution Architecture Management is to support the delivery of specific change projects; to review architecture decisions and migration plans to identify efficiencies and advance standardisation; to ensure the solutions align to the architecture and technology principles, policies, standards and reference models defined by TS Enterprise Architecture Management processes; and capture and manage exceptions.
- 8.3.4 The purpose of TS Deployed Architecture Management is to provide an up to date, consistent baseline of information about the provision of the End to End Services; to contribute to the integrated change planning process from demand to delivery; and to ensure compliance with and alignment to the Authority's Enterprise Architecture. TS Deployed Architecture Management facilitates alignment of the Deployed Architecture for the Transitional Services (TS Deployed Architecture) with Authority business objectives and operating models.
- 8.3.5 The Service Requirements for TS Architecture Management are listed below:

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	TS Enterprise Architecture Management
8.3.5.1	3	The Supplier shall provide Enterprise Architecture Management Transitional Services for their environments as contracted and ensure these are aligned to Good Industry Practice.
8.3.5.2	3	The Supplier shall work and collaborate with the Authority and the Other Suppliers (where required to do so) to collate their aspects of the Transitional Services and TS Deployed Architecture and make it available to the Authority
8.3.5.3	3	The Supplier shall provide full details of any tools and methods they reference in Project Proposals, where such tools and/or methods are not described in publicly available standards.
	2	TS Deployed Architecture Management
8.3.5.4	3	The Supplier shall ensure that the TS Deployed Architecture service is compliant with the agreed TS Service Operations Manual.
8.3.5.5	3	The Supplier shall provide TS Documentation to describe the TS Deployed Architecture to the Authority within three (3) months of the Transitional Services Commencement Date.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
8.3.5.6	3	<p>The Supplier shall update and maintain the TS Documentation to describe the TS Deployed Architecture not less than annually following the Transitional Services Commencement Date, and make the updates available to the Authority within one (1) Working Day of the update being agreed by the Authority. The Supplier shall provide the Authority with access to TS LLDs to the extent required:</p> <p class="list-item-l1">(a) for the Authority to benefit from the Transitional Services; and</p> <p class="list-item-l1">(b) to enable the transition of the delivery of the Transitional Services from the Supplier to the Authority.</p>
8.3.5.7	3	The Supplier shall provide TS Deployed Architecture in accordance with the Architecture Standard set out in Paragraph 11.1 of Annex 4 (<i>TS Standards</i>) and submit this for Approval in accordance with the Document Approval Procedure twice per year by January 1st and July 1st.
8.3.5.8	3	The Supplier shall update the Approved TS Deployed Architecture to the Architecture Standards set out in Annex 4 (<i>TS Standards</i>) not less than quarterly and make it available to the Authority.
8.3.5.9	3	The Supplier shall provide TS Deployed Architecture with a forecast for the reasonably foreseeable future of the Transitional Services, describing any change that may be required for a Service in order to maintain business operation, in accordance with the Architecture Standards set out in Annex 4 (<i>TS Standards</i>) and submit this for Approval twice per year by January 1st and July 1st, unless otherwise agreed by the Authority.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
8.3.5.10	3	The Supplier shall perform Architecture Impact Assessment upon the TS Deployed Architecture to ensure ongoing manageability and supportability of the live environment in accordance with the TS Change and Evaluation Management Processes as set out in the agreed TS Service Operations Manual
	2	Solution Architecture Management
8.3.5.11	3	The Supplier shall ensure that the provided Solution Architecture for the Transitional Services (TS Solution Architecture) is compliant with the Architecture Standards set out in Annex 4 (TS <i>Standards</i>) and Good Industry Practice.
8.3.5.12	3	The Supplier shall, at the request of the Authority, provide input to the production and assessment of architecture requirements and solution options, providing technical input into solution estimation.
8.3.5.13	3	The Supplier shall, at the request of the Authority, provide input to the production of TS Solution Architectures that cover the domains of all relevant Other Suppliers and the specific Technical Architectures within the Transitional Services. The Transitional Services shall include assessment and recommendation of the most appropriate implementation and migration planning approach.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Architecture Governance
8.3.5.14	3	The Supplier shall ensure that the provided Architecture Governance for the Transitional Services is compliant with the Architecture Standards set out in Annex 4 (<i>TS Standards</i>) and Good Industry Practice.
8.3.5.15	3	The Supplier shall participate in all relevant architecture governance activities and forums, including relevant forums and boards described in Schedule 21 (<i>Governance</i>) and the agreed TS Service Operations Manual. The activities and forums for architecture governance will address all aspects of architecture delivery, including but not limited to; i) TS Enterprise Architecture Governance; ii) TS Solution Architecture Governance; and iii) TS Deployed Architecture Governance.
8.3.5.16	3	The Supplier shall comply with the consolidated Deployed Architecture Standards, collated by the Authority, when providing services to be hosted within the IT environments of Other Suppliers, unless otherwise agreed by the Authority.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
8.3.5.17	3	The Supplier shall ensure that all Approved Service Architecture artefacts comply with the relevant Architecture Standards set out in Annex 4 (TS <i>Standards</i>) and are made available to the Authority in accordance with the agreed TS Service Operations Manual.
8.3.5.18	3	The Supplier shall work and collaborate with the Authority to ensure that any Approved architectural dispensations, waivers, risks, issues and assumptions assigned to the Supplier are managed in accordance with the TS Standards set out in the agreed TS Service Operations Manual.
8.3.5.19	3	The Supplier shall work and collaborate with the Authority in the ongoing assessment and development of the Architecture Management capability of the Transitional Services.
8.3.5.20	3	The Supplier shall provide architectural leadership in relation to the Transitional Services, providing strategy and direction to the Authority, and Other Suppliers on the request of the Authority.
8.3.5.21	3	The Supplier shall provide and maintain a catalogue of services from which the Authority can request the provision of architectural expertise in the architecture of Transitional Services or other architecture domains. The expertise shall align to the Skills Framework for the Information Age (SFIA) version 5 or later.

8.4 TS Licence Management and Compliance

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 8.4.1 This section sets out the requirements in relation to Supplier's adherence to the applicable terms and conditions for TS Licensed Software.
- 8.4.2 The Service Requirements for TS Licence Management and Compliance are listed below:

Requirement No.	Level	Requirement
	2	General Requirements
8.4.2.1	3	The Supplier shall be responsible for the provision and renewal of all licences for TS Licenced Software in accordance with Clause 3.2(j) (Warranties).
8.4.2.2	3	The Supplier shall be responsible for the ongoing management and monitoring of licence usage in order to ensure that such usage is both legal and efficient, including the enablement of licence redeployment to minimise licence costs.

**APPENDIX A (TS SERVICE MANAGEMENT REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

End of annex

**ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Annex 2 (Transitional Services Description)

Appendix B

TS Technical Requirements

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

1 TECHNICAL INFRASTRUCTURE SERVICES

1.1 Environments

1.1.1 This is the provision of a range of TS IT Environments to support the testing and delivery of services to support the Transitional Services. Current services are provisioned with different levels of security administered and include:

- (a) connectivity to allow access to systems and data classified as OFFICIAL (including where also marked “-SENSITIVE”) from appropriate devices;
- (b) connectivity to allow access to selected systems and data classified as OFFICIAL from appropriate devices (typically kiosks and IT for prisoners and people on probation);
- (c) connectivity to allow access to the Authority System and Authority Data over the internet (typically classified as OFFICIAL); and
- (d) provision and management of connectivity test environments to support testing.

1.1.2 The TS Technical Requirements for “Environments” are listed below:

Requirement No.	Level	Requirement
	2	Live Environments
1.1.2.1	3	The Supplier shall provide, maintain, and support the service components of live environments to support the delivery of the End to End Services.

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
1.1.2.2	3	The Supplier shall work and collaborate with the Authority and Other Suppliers, to ensure Live Environments for delivery of the End to End Services are fully functional.
1.1.2.3	3	The Supplier shall ensure that the provisioning and maintenance of the Transitional Service components of the Live Environments, where appropriate, meet the requirements in Annex 4 (<i>TS Standards</i>) and Annex 5 (<i>Security Management</i>).
1.1.2.4	3	The Supplier shall work and collaborate with Other Suppliers to provide, maintain and support Live Environments to support the delivery of End to End Services.
1.1.2.5	3	The Supplier shall only use hosting components available through the TS Product and Service Catalogue for services delivered by Other Suppliers unless otherwise agreed by the Authority.
	2	Non-Live Environments
1.1.2.6	3	The Supplier shall provide, manage and maintain the service components of non-live environments to support the delivery of the End to End Services.
1.1.2.7	3	The Supplier shall work and collaborate with the Authority and Other Suppliers, to establish Non-Live Environments when required to support the delivery of the End to End Services.

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
1.1.2.8	3	The Supplier shall ensure that the provisioning and maintenance of the Transitional Services components of the Non-Live Environments, where appropriate meets the requirements in Annex 4 (TS <i>Standards</i>) and Annex 5 (<i>Security Management</i>).
1.1.2.9	3	The Supplier shall manage, monitor and maintain the Authority's non-live environment for the TS Gateway (the "TS Gateway Test System") to enable testing (e.g. of the Authority's end user compute platform and devices).
1.1.2.10	3	The Supplier shall make the TS Gateway Test System available to Other Suppliers and/or the Authority's and Service Recipients' testers.
1.1.2.11	3	The Supplier shall, where required by the Authority, disconnect all relevant equipment operating in the TS Gateway Test System from the Master Time Reference service to enable testing to be performed.

1.2 Data Centre Facilities Service

1.2.1 The TS Technical Requirements for "Data Centre Facilities Service" are listed below:

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	General Requirements
1.2.1.1	3	The Supplier shall use the data centre facilities provided to the Supplier by the Authority's data centre supplier (" Data Centre Facilities ").
1.2.1.2	3	The Supplier shall provide any necessary change to requirements for hosting of non-rack mounted equipment to the Authority's data centre Other Supplier with ten (10) Working Days' notice.
1.2.1.3	3	The Supplier shall use the equipment build and test areas (of a size no less than five (5) metres wide, four (4) metres deep and two and a half (2.5) metres high) provided to the Supplier by the Authority's data centre supplier for the building and testing of ICT equipment.
1.2.1.4	3	The Supplier shall ensure the Supplier Personnel who attend the Authority's data centre supplier's Facilities attend training courses prior to their commencement of work at the Data Centre Facilities.

1.3 Public Key Infrastructure

- 1.3.1 The Supplier shall provide, maintain and support a PSN Standard-compliant Public Key Infrastructure (PKI) and encryption management service in accordance with the applicable TS Standards set out in Annex 4 (TS *Standards*) solely to support the WAN provided under the Transitional Services (the "**PKI Service**").

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 1.3.2 The PKI Service shall be established in line with the PSN Standard and provide the necessary cryptographic services to support the Authority's connection to the PSN Inter-Provider Encryption Domain (IPED) and an Authority's private wide area network.
- 1.3.3 The PKI Service will be used to provide the Transitional Services provided by the Supplier.
- 1.3.4 The PKI Service will be operated by authorised crypto custodians in accordance with HMG policy.
- 1.3.5 The TS Technical Requirement for the PKI Service is listed below:

Requirement No.	Level	Requirement
	2	General Requirement
1.3.5.1	3	The Supplier shall deliver the Transitional Services that utilise PKI services in accordance with the Public Key Cryptographic Standards (PKCS).

2 NETWORK INFRASTRUCTURE SERVICES

2.1 Core Network Services

2.1.1 Core Network Services integrate a number of key network services for the Authority's end to end environment including:

- (a) **"IP Address Management"**: the process and technology involved in defining IP schemas, allocating IP addresses to devices on a dynamic / reserved / fixed basis (e.g. through the implementation of Dynamic Host Configuration Protocol services), and ensuring that unused addresses are available to be used by other devices. The internal IP addresses assigned for the Transitional Services are for the Authority's use only. The addressing of the underlying infrastructure is as per the PSN Standards as listed in Annex 4 (TS Standards);

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) **"Master Time Reference"**: often required for transaction/replication services, time services provide access to a trusted time source to synchronise the various components of the End to End Services;
- (c) **"External Domain Name Service (DNS)"**: translates queries for domain names into IP addresses; and
- (d) **"Network Optimisation"**: provides a number of sub-services (including traffic marking) which allows the prioritisation of network traffic.

2.1.2 The TS Technical Requirements for Core Network Services are listed below:

Requirement No.	Level	Requirement
	2	IP Address Management
2.1.2.1	3	The Supplier shall deliver the Transitional Services in accordance with the Authority's IP Addressing policy.
2.1.2.2	3	The Supplier shall request from the Authority IP address ranges for the provision of the Transitional Services.
2.1.2.3	3	The Supplier shall manage the allocation of IP addresses to deliver the Transitional Services.
2.1.2.4	3	The Supplier shall ensure that all IP addresses used within its infrastructure are either RFC 1918 addresses or officially registered to the Authority.
2.1.2.5	3	The Supplier shall use the dynamic IP address allocation service provided by Other Suppliers for the allocation of IP addresses to support devices connected at Sites.

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
2.1.2.6	3	The Supplier shall work and collaborate with Other Suppliers to provide any device configuration information that is required to be applied by the Other Supplier of dynamic IP address allocation services.
2.1.2.7	3	The Supplier shall work and collaborate with Other Suppliers to ensure that the Other Supplier of dynamic IP address allocation services can register devices with the Domain Naming Service (as described below).
	2	Master Time Reference
2.1.2.8	3	The Supplier shall use a Master Time Reference and use a stratum three (3) time source in the delivery of the Transitional Services.
2.1.2.9	3	The Supplier shall ensure that devices used in the delivery of the Transitional Services are within one (1) second of the Master Time Reference.
	2	Domain Naming Service
2.1.2.10		The Supplier shall provide a DNS proxy service which resolves PSN-A, PSN-P and Internet namespace.
2.1.2.11	3	The Supplier shall be responsible for registering with the Other Suppliers any internal DNS records required to deliver the Transitional Services.

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
2.1.2.12	3	The Supplier shall work and collaborate with the Other Suppliers where required to ensure that DNS services for the Authority provide fully functional DNS resolution for the provision of the End to End Services.
	2	Network Performance Optimisation
2.1.2.13	3	The Supplier shall provide, manage and maintain a PSN Standard-compliant Quality of Service (QoS) model to enable the prioritisation of the Authority's network traffic across the network infrastructure to support the delivery of the End to End Services. The QoS Model shall be made available to the Authority at any time upon request and in any case within forty (40) Working Days of any change to the QoS model.
2.1.2.14	3	The Supplier shall implement Quality of Service (QoS) in accordance with the PSN Standard and Service Classes, unless otherwise agreed with the Authority.
2.1.2.15	3	The Supplier shall coordinate the implementation of Quality of Service (QoS) technologies in collaboration with the Authority and Other Suppliers to ensure the delivery of the End to End Services to the required TS Service Levels as set out in Annex 3 (<i>TS Performance Levels</i>).
2.1.2.16	3	The Supplier shall, where required, work and collaborate with the Authority and Other Suppliers, to assign prioritisation and bandwidth parameters to the Transitional Services to support the delivery of the End to End Services to the required TS Service Levels as set out in Annex 3 (<i>TS Performance Levels</i>).

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
2.1.2.17	3	The Supplier shall implement Quality of Service (QoS) with a minimum of three (3) levels: i) expedited forwarding (EF); ii) assured forwarding (AF); iii) default.
	2	Encryption Services
2.1.2.18	3	The Supplier shall ensure that all cryptographic Services comply with the TS Standards set out in Annex 4 (TS <i>Standards</i>) and use devices that have NCSC or relevant CPA assurance unless otherwise agreed with the Authority.
2.1.2.19	3	The Supplier shall manage an encryption service to support the PSN WAN Services (Private VPN Service) in compliance of Annex 5 (<i>Security Management</i>) (the “ Encryption Services ”).
2.1.2.20	3	The Supplier shall implement and provision the Encryption Services in accordance with the design agreed between the Parties under the Preceding Services, subject to compliance with Annex 5 (<i>Security Management</i>).
2.1.2.21	3	The Supplier shall provide, manage and maintain assured separation between Live, Non-Live, external and legacy IT environments in compliance of Annex 5 (<i>Security Management</i>).

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
2.1.2.22	3	The Supplier shall provide manage and maintain a PSN compliant Wide Area Network service to Authority Sites that ensures assured cryptographic separation from all other PSN Environments in accordance with the Authority risk assessment, Authority, PSN and HMG policy.
2.1.2.23	3	The Supplier shall connect Sites to the WAN provided under the Transitional Services using a cryptographic overlay in accordance with the Security standards set out in Annex 4 (Standards).

2.2 WAN

- 2.2.1 The Supplier shall provide key infrastructure to support the End to End Services including:
- (a) **"PSN WAN Services (Private VPN Service)"**, being the core infrastructure and WAN circuits:
 - (i) to provide connectivity to Authority Sites and other sites nominated by the Authority in accordance with the PSN Standard; and
 - (b) **"Broadband and Mobile Services"**, being provision of:
 - (i) broadband capability; and
 - (ii) mobile broadband capability including data;

to specified Sites or Extended Locations and/or nominated individuals.

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

2.2.2 The Transitional Services provide the infrastructure and services to enable a separation between voice and data in accordance with the PSN Standard and other relevant TS Standards.

2.2.3 The TS Technical Requirements which shall apply to Paragraphs 2.2.1 and 2.2.2 are listed below:

Requirement No.	Level	Requirement
	2	PSN WAN Services (Private VPN Service)
2.2.3.1	3	The Supplier shall ensure that packet loss shall occur less than once for every two thousand (2,000) packets transmitted to the required TS Service Levels set out in Annex 3 (<i>TS Performance Levels</i>).
2.2.3.2	3	The Supplier shall ensure that the round trip delay for packets transmitted across the Network, between the LAN port of the Supplier's customer equipment at one Site to the LAN port of the Supplier's customer equipment at another Site, shall be less than fifty (50) milliseconds, subject to the traffic being marked as PSN Real Time CoS and for bandwidths greater than forty-five (45) Mbps.
2.2.3.3	3	Subject to the availability of existing fibre the Supplier shall ensure that for Site connections at or below ten (10) Gbps the connection shall be implemented within forty-five (45) Working Days of receipt of a relevant Project Request.

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
2.2.3.4	3	Where existing fibre is not present the Supplier shall ensure that for Site connections at or below ten (10) Gbps the connection shall be implemented within ninety (90) Working Days of receipt of a relevant Project Request, including all preparation work.
2.2.3.5	3	The Supplier shall work and collaborate with the Authority and Other Suppliers to facilitate the connection of the Service to Other Suppliers' LAN to support the delivery of the End to End Services.
2.2.3.6	3	The Supplier shall monitor, manage and maintain any cabling up to the CPE on Authority Sites to minimise cabling faults and failures.
2.2.3.7	3	The Supplier shall ensure that all Software used on Network Devices implemented in the ICT Environment used for the delivery of the Transitional Services is not more than five (5) years old and has at least three (3) years support available [REDACTED]
2.2.3.8	3	The Supplier shall work and collaborate with the Authority and the appropriate Government bodies, where the Authority Site is a listed building or where planning consent is required to carry out cabling work.
2.2.3.9	3	The Supplier shall work and collaborate with the Authority and the appropriate Government bodies, where the Authority Site is a rented building or where planning consent is required to carry out cabling work.

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
2.2.3.10	3	The Supplier shall ensure they are compliant with the terms of the PSN connectivity framework and shall provide a copy of their PSN compliance certificates on an annual basis following the Effective Date.
2.2.3.11	3	The Supplier shall provide a cryptographic overlay for the Services that is compliant with the security standards set out in Annex 4 (TS <i>Standards</i>)
	2	Broadband and Mobile Services
2.2.3.12	3	The Supplier shall provide the following elements of the Broadband and Mobile Services individually or in any combination: i) pre-configured broadband devices; ii) installation and testing at the End User's Extended Location, iii) broadband connection (line); and iv) Installation and configuration instructions for the End User.
2.2.3.13	3	The Supplier shall provide, maintain and support a Broadband and Mobile Service to nominated End Users or groups at specified Extended Locations to enable access to the End to End Services via the Internet.

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
2.2.3.13B		The Supplier shall provide its proprietary enterprise broadband solution (“VEB”) for Unpaid Work Sites (UWS).
	2	Internet Connectivity Service
2.2.3.14	3	The Supplier shall provide, manage and maintain Internet connectivity to Authority's Data Centre Facilities and the Supplier's data centre facilities used for the provision of the End to End Services. This shall include provision of the Authority edge (CE) router.
2.2.3.15	3	The Supplier shall make available on the TS Product and Service Catalogue the provision, management and maintenance of Internet connectivity. This shall include the Authority edge (CE) router where required by the Authority.

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
2.2.3.16	3	The Supplier shall work and collaborate with Other Suppliers to implement the TS Gateway and the required security controls for the Internet connectivity Service in accordance with the Authority's IT IA policies, processes and procedures.
2.2.3.17	3	The Supplier shall ensure the Internet connectivity meets the bandwidth, availability and other service levels as set out in Annex 3 (TS <i>Performance Levels</i>).

2.3 "Direct Internet Access (DIA) Services" (IPSec VPN Service)

2.3.1 The Supplier shall:

- (a) provide dedicated internet access (DIA) circuits ; and
- (b) maintain the Authority's [REDACTED]

in accordance with the following requirements:

Internet Requirements		
Requirement No		Requirement
	2.3.1.1	Provision of Internet connectivity at all probation and probation reform sites as required by the Authority Internet using IPv4 and Ipv6 public addressing presented on a switch that can be shared by multiple users of the site/location.
	2.3.1.2	Provide the following Resilience Options: i. Single. A single circuit, one (1) Gbps Bearer, with a starting bandwidth of two hundred (200) Mbps.

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

		ii. Dual. A resilient circuit, from one supplier with one (1) Gbps bearer, with a starting Internet bandwidth of four hundred (400) Mbps. Resilience must be to diverse points of presence, with any building entry pinch points identified and documented.
	2.3.1.3	Internet access is via the local Internet circuit(s), and never tunnelled elsewhere.
	2.3.1.4	[Ensure the local firewall acts as a DNS proxy and sends all DNS requests to the NCSC's 'Protective Domain Name Service'.]
	2.3.1.5	[Ensure all event logs for access to the network and firewall policy rules are sent to the Authority's SOC/SIEM service.]
	2.3.1.6	Monitor system dashboard of usage and volumetrics of all equipment.
	2.3.1.7	Provide "MoJ-AV" service
899-017		The Supplier shall ensure that VPN service terminates traffic into the TS Gateway for onward routing to the rest of the network
899-018		The Supplier shall ensure connectivity to the Authority System from a Site over the internet is in compliance with Annex 5 (<i>Security Management</i>) and NCSC recommended IPSEC cryptographic profiles and specifications.
899-021	2.3.1.8	The Supplier shall create all Site VPNs from the Site to the hubs. Any site-to-site traffic such as telephony or video will go via the hubs. Telephony will be based on Microsoft Teams where calls are anchored in Microsoft Office 365
	2.3.1.9	The Supplier shall ensure that public internet access is filtered through a local firewall utilising web filtering technology, without reliance on an explicit forward proxy configuration, and whereby user identification shall be enabled, and all associated event logs shall be transmitted to the Authority's logging platform.
	2.3.1.10	The Supplier shall ensure that the Direct Internet Access (DIA) Services meets the TS Service Levels as set out in Annex 3 (TS Performance Levels)
	2.3.1.11	The Supplier should specify each Authority Site's to router to optimise the bearer speed without uplift in ISP hardware (e.g. 1 Gbps bearer should be connected to a router capable of handling 1 Gbps traffic, regardless of CDR)
	2.3.1.12	The Supplier shall offer a range of Internet circuit options:

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

		1. Field sites (under 25 users) – 200/1000Mbps 2. Small sites (26-100 users) – 400/1000Mbps 3. Medium site (101 -250) – 1000/10000Mbps

2.3.2 For the following Authority Sites (“**Digital Prison Sites**”), the Supplier shall provide DIA circuits to the specification of Paragraph 2.3.1, save sub-paragraphs 2.3.1.4 and 2.3.1.5:

- HMP Chelmsford
- HMP Eastwood Park
- HMP Exeter
- HMP Guys Marsh
- HMP Leeds
- HMP Liverpool
- HMP Moorlands
- HMP Nottingham

2.4 TS Gateway

2.4.1 These services include managed gateway services; gateway infrastructure; provision of all elements of a complete solution including gateway services between; protected and secure systems and the internet; Government secure systems and industry secure systems; departmental controlled systems at different security levels; different UK Government departmental secure systems; UK Government departmental secure

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

systems and secure systems of allied nations; remote access gateways; Government and business services (e.g. electronic commerce, purchase to pay systems, human resources systems etc.)

2.4.2 The TS Gateway provides a set of controls and security mitigations to protect the TS IT Environment. A set of gateways is required to support the End to End Services:

- (a) **"Management Gateways"** that support remote management of systems in the delivery of the End to End Services;
- (b) Network Interconnect to support many to many interactions between multiple networks;
- (c) **"Interoperability Gateway"** to demarcate the boundary of two or more environments that have different risk profiles or Accreditation scopes and manage information assets at the same impact level or protective marking; and,
- (d) **"Inter-Domain Gateway"** to demarcate the boundary of two or more environments that have different risk profiles or accreditation scopes and manage information assets at different impact levels or protective marking.

2.4.3 The benefits to the Authority of a managed set of secure gateways shall include the following:

- (a) complexity reduction, through a small, discrete set of reusable facilities rather than many point-to-point capabilities; and
- (b) improved security posture through a less complex managed set of facilities.

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	General Requirements
2.4.3.1	3	The Supplier shall design, provide, maintain and support the TS Gateway to enable controlled connectivity between IT environments. The Supplier shall implement security controls as required under Annex 5 (<i>TS Security Management</i>) and in compliance with the standards set out in Annex 4 (<i>TS Standards</i>).
2.4.3.2	3	The Supplier shall provide, maintain and support the TS Gateway as required for the delivery of the Transitional Services.
2.4.3.3	3	The Supplier shall provide, maintain and support the TS Gateway within the Data Centre Facilities provided by the Authority's Data Centre Supplier, and at Authority Sites as required, to provide common security controls required for the delivery of services by the Other Suppliers.
2.4.3.4	3	The Supplier shall provide the facility for Other Suppliers to integrate, provide, maintain and support security controls specific to those Other Suppliers' services, within the TS Gateway.
2.4.3.5	3	The Supplier shall integrate, provide, maintain and support security controls specific to the Transitional Services within the TS Gateway, in compliance with Annex 5 (<i>TS Security Management</i>) and the standards set out in Annex 4 (<i>TS Standards</i>).

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
2.4.3.6	3	The Supplier shall work and collaborate with relevant Other Suppliers to ensure that where such Other Supplier are using internet connectivity via the Transitional Services, the connectivity is fully functional and meets the TS Service Levels as set out in Annex 3 (<i>TS Performance Levels</i>).
	2	Interoperability Gateways
2.4.3.7	3	The Supplier shall provide, manage and maintain Interoperability Gateways between the Authority System’s environments and other IT environments that are accredited to protect information assets at the same protective marking, including the following types of environment: (i) other environments within Authority System; (ii) Other Suppliers’ IT environments; (iii) Public Services Network (PSN); and (iv) other external IT environments. The security controls to be implemented at an Interoperability Gateway shall be set out in the TS Security Management Plan.

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
2.4.3.8	3	The Supplier shall provide the facility for the Other Suppliers to integrate, provide, maintain and support security controls specific to those Other Suppliers' services, within the Interoperability Gateways provided by the Supplier, in compliance with Annex 5 (<i>TS Security Management</i>) and the standards set out in Annex 4 (<i>TS Standards</i>).
2.4.3.9	3	The Supplier shall integrate, provide, maintain and support security controls specific to the Authority's voice and video Services within the Interoperability Gateways provided by the Supplier, in compliance with Annex 5 (<i>TS Security Management</i>) and the standards set out in Annex 4 (<i>TS Standards</i>).
	2	Inter-Domain Gateways

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
2.4.3.10	3	The Supplier shall provide, manage and maintain Inter-Domain Gateways between IT environments that are accredited to protect information assets at different protective markings, including the following types of environment: (i) Authority System; (ii) Other Suppliers' IT environments; (iii) Public Services Network (PSN); and (iv) Other Suppliers. The security controls to be implemented at an Inter-Domain Gateway shall be set out in the TS Security Management Plan.
2.4.3.11	3	The Supplier shall provide the facility for Other Suppliers to integrate, provide, maintain and support security controls specific to such Other Suppliers' respective services, within the Inter-Domain Gateways provided by the Supplier, in compliance with the standards and requirements set out in Annex 5 (<i>TS Security Management</i>) and Annex 4 (<i>TS Standards</i>).
2.4.3.12	3	The Supplier shall integrate, provide, maintain and support security controls specific to the Transitional Services within the Inter-Domain Gateways provided by the Supplier, in compliance with the standards and requirements set out in Annex 5 (<i>TS Security Management</i>) and Annex 4 (<i>TS Standards</i>).

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
	2	Management Gateway Service
2.4.3.13	3	The Supplier shall provide maintain and support a remote access service to enable Other Suppliers to access management IT environments within the Data Centre Facilities provided by the Authority's data centre supplier and Authority Sites, from the Internet or Public Services Network (PSN), and this access shall provide: [REDACTED] [REDACTED] [REDACTED] [REDACTED] (v) All Inter Domain and Interoperability Gateways required to support the service. Such services shall be provided in compliance with Annex 5 (<i>TS Security Management</i>) and the standards set out in Annex 4 (<i>TS Standards</i>).
2.4.3.14	3	The Supplier shall make access to management IT Environments within the Data Centre Facilities provided by the Authority's data centre supplier, and Authority Sites, available to Other Suppliers through the TS Product and Service Catalogue.

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
2.4.3.15	3	The Supplier shall provide maintain and support the security controls required to control management access to the Transitional Services hosted within the Data Centre Facilities provided by the Authority's data centre supplier, including but not limited to: [REDACTED] These controls shall be provided in compliance with Annex 5 (<i>TS Security Management</i>) and the standards set out in Annex 4 (<i>TS Standards</i>).
2.4.3.16	3	The Supplier shall enable controlled access to the IT Environment via the TS Gateway to the Authority and Other Suppliers as requested in writing and authorised by the Authority for the purposes of supporting the End to End Services.

2.5 Network Integration Services

2.5.1 "Network **Integration Services**" shall include but not be limited to:

- (a) ensuring compliance with PSN standards;
- (b) physical and logical design of the Transitional Services, including the integration of multiple separate networks;
- (c) technical integration of the Transitional Services to ensure TS Service Levels are met; and
- (d) ensuring that the Transitional Services are presented and managed as a seamless service to the Authority and the Other Suppliers;

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

2.5.2 The TS Technical **Requirements for Network Integration Services** are listed below:

Requirement No.	Level	Requirement
	2	General Requirements
2.5.2.1	3	The Supplier shall work and collaborate with Other Suppliers in the delivery of End to End Services requiring the technical integration of Transitional Services with services provided by Other Suppliers.
2.5.2.2	3	The Supplier shall work and collaborate with the Authority and Other Suppliers to ensure the TS Gateway is fully functional.
2.5.2.3	3	The Supplier shall provide a Network Integration Service with a single point of responsibility for integrating multiple networks for the provision of End to End Services, including but not limited to: (i) the physical and logical network design for the integration of multiple separate networks, as required by the Authority. This shall provide the seamless integration and transmission of traffic between the connected networks; (ii) the physical and logical network design for the separation of Live and Non-Live Environments; and (iii) physical or logical separation of ICT Environments handling information assets at different protective markings.

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
2.5.2.4	3	The Supplier shall provide a Network Integration Service to ensure that the Transitional Services are delivered in accordance with the TS Service Levels, TS Service Level Targets and KPIs set out in Annex 3 (TS <i>Performance Levels</i>).
2.5.2.5	3	The Supplier shall maintain an internet connectivity high-level design.
	2	Network Interconnect Services
2.5.2.6	3	The Supplier shall work and collaborate with the Authority to (where agreed via the Change Control Procedure) procure a Network Interconnect Service with a single point of responsibility for the integration of multiple separate networks, as required by the Authority. This shall provide the seamless integration and transmission of traffic for the provision of End to End Services, including but not limited to: i) maintaining Quality of Service (QoS) prioritisation of network traffic across the Network Interconnect Service; ii) efficient and resilient network routing of Authority data across the networks that are connected to the Network Interconnect Service; and iii) management of IP Address conflicts and, where required, network address translation when integrating multiple networks.

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Requirement No.	Level	Requirement
2.5.2.7	3	The Supplier shall work and collaborate with the Authority and Other Suppliers to ensure that where such Other Suppliers' services are using the Network Interconnect Service, such services are enabled by the Transitional Services as reasonably required to deliver such services to their respective performance standards.
2.5.2.82.5.2.8	3	The Supplier shall procure the Network Interconnect Service availability to Other Suppliers for the provision of End to End Services.
2.5.2.9	3	The Supplier shall provide, manage and maintain the required TS Gateway to implement the Network Interconnect Service. This shall include the provision of Interoperability Gateways and Inter-Domain Gateways in compliance with the standards and requirements set out in Annex 5 (<i>TS Security Management</i>) and Annex 4 (<i>TS Standards</i>).
2.5.2.10	3	The Supplier shall provide a Network Interconnect Service with a resilient technical architecture to support the provision of the Transitional Services across the Network Interconnect Service, to meet the TS Service Levels as set out in Annex 3 (<i>TS Performance Levels</i>).

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]
[REDACTED]

[REDACTED] [REDACTED]
[REDACTED]

[REDACTED] [REDACTED]
[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]
[REDACTED]
[REDACTED]

**APPENDIX B (TS TECHNICAL REQUIREMENTS) to
ANNEX 2 (TRANSITIONAL SERVICES DESCRIPTION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

End of Annex

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 3

TS PERFORMANCE LEVELS

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

1A DEFINITIONS

1A.1 For the purposes of this Schedule 34, the following definitions shall apply:

“Critical TS Service Failure”	a failure identified as a critical service failure in this Annex 3 (<i>TS Performance Levels</i>);
“Escalation Process”	the initial stages of the process for dealing with Disputes without the intervention of third parties as set out in Paragraphs 2 and 4 of Schedule 23 (<i>Dispute Resolution Procedure</i>);
“Exception Report”	the report issued by the Supplier in accordance with Paragraphs 6.3(a) and/or 6.4(b) of this Annex 3 (<i>TS Performance Levels</i>), which shall provide details of actions taken by the Supplier to resolve the TS Incident and plans to avoid any further repeated TS Incidents;
“Incident Resolution”	the action taken to repair the cause(s) of a TS Incident or to implement a workaround to the satisfaction of the Authority;
“Incident Resolution Priority”	the incident resolution priority categories set out in Table 2 (TS Incident Severity Levels and Definitions) of this Annex 3 (<i>TS Performance Levels</i>);
“Incident Resolution Time”	the time taken to achieve Incident Resolution in accordance with Paragraph 3.4(g)(i) of this Annex 3 (<i>TS Performance Levels</i>);
“Material TS Service Level Failure”	a failure identified as a material service level failure in this Annex 3 (<i>TS Performance Levels</i>);
“Other Resolver Group”	means any Other Supplier who has responsibility for the resolution of events, incidents or problems;
“Recovery Plan”	a plan prepared by the Supplier in accordance with Paragraph 6 of this Annex 3 (<i>TS Performance Levels</i>), which shall provide details of the remedial actions and activities to be undertaken by the Supplier and the recovery period in respect of the relevant TS Service Level Failure;
“RPO”	Recovery Point Objective;

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“RTO”	Recovery Time Objective;
“Security Incident”	shall have the meaning given in Schedule 1 (Definitions);
“Security Incident Management”	the monitoring and detection of Security Incidents;
“Security Incident Resolution Plan”	a plan of actions agreed with the Authority to investigate, diagnose, resolve, and prevent future occurrences of a Security Incident;
“Security Incident Severity”	the severity assigned to those categories of Security Incident set out in Table 3 (Security Incident Severity Definitions) in this Annex 3 (<i>TS Performance Levels</i>);
“Severity”	a category used to identify the relative importance of a TS Incident, problem or change based on the impact on the Authority’s productivity as a result of a reduction or loss of TS Service Availability or performance of an aspect of the Transitional Services, including the categories described in this Annex 3 (<i>TS Performance Levels</i>);
“Service Measurement Period”	the period over which a TS Performance Level is measured (for example, monthly, quarterly or annually) as set out in Appendix A to this Annex 3 (<i>TS Performance Levels</i>);
“Service Performance Management”	the services to be provided by the Supplier to manage the performance of the Transitional Services, as described by this Annex 3 (<i>TS Performance Levels</i>);
“TS Incident”	a TS Service Incident or a Security Incident’
“TS Incident Management System”	an automated system used to track and manage the status of records of TS Incidents defined and maintained throughout the TS Incident lifecycle;
“TS Key Performance Indicator” or “TS KPI”	a key performance indicator set out in Paragraph 4 of Appendix A to this Annex 3 (<i>TS Performance Levels</i>);

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“TS KPI Target”	the target for a TS KPI set out in the relevant table in Appendix A of this Annex 3 (<i>TS Performance Levels</i>);
“TS Management Information”	the management information specified in Annex 3 (<i>TS Performance Levels</i>), Annex 15 (<i>TS Charges and Invoicing</i>) and Schedule 21 (Governance) to be provided by the Supplier to the Authority;
“TS Performance Levels”	means the TS Service Levels and the TS KPIs;
“TS Service Availability”	has the meaning given in Paragraph 2.2(b) of this Annex 3 (<i>TS Performance Levels</i>);
“TS Service Credit Point”	a point accrued in respect of the Supplier’s failure to deliver a TS Service Line in accordance with an applicable TS Service Level Target set out in this Annex 3 (<i>TS Performance Levels</i>);
“TS Service Credit Regime”	the regime for TS Service Credits set out in Paragraph 4 of this Annex 3 (<i>TS Performance Levels</i>);
“TS Service Hour”	the service and support hours applicable to each TS Service Line as set out in Table 1 in Paragraph 2.2(e) of this Annex 3 (<i>TS Performance Levels</i>);
“TS Service Incident”	a reported occurrence of an unplanned interruption to or reduction in the quality of any part of the Transitional Services in accordance with the Authority TS Requirements or the TS Performance Levels;
“TS Service Level”	the service levels set out in Paragraphs 1, 2 and 3 of Appendix A to this Annex 3 (<i>TS Performance Levels</i>);
“TS Service Level Failure”	a failure to meet a TS Service Level Target in respect of a TS Service Level;
“TS Service Level Target”	the target for a TS Service Level as described in Appendix A of Annex 3 (<i>TS Performance Levels</i>) or, where a TS KPI is promoted to a TS Service Level, the relevant TS KPI Target;

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

“TS Service Level Threshold”	the threshold for a TS Service Level as described in Paragraph 3.1(c) of this Annex 3 (<i>TS Performance Levels</i>);
“TS Service Line”	a service line identified in Table 1 (<i>TS Service Availability Hours and TS Service Hours</i>) in Paragraph 2.2(e) of this Annex 3 (<i>TS Performance Levels</i>);
“TS Service Unavailability”	in relation to the Authority System and the Supplier TS System or the Transitional Services, any period of time that there is no TS Service Availability of the Authority System and the Supplier TS System or the Transitional Services; and for the purposes of this Schedule 34 “TS Unavailability” shall be construed accordingly;
“Threat”	threats include viruses, trojans, phishing and all other possible risks to the Transitional Services;
“Unavailable” or “TS Unavailability”	has the same meaning as “TS Service Unavailability”;
“VIP Sites(s)”	has the meaning given in Paragraph 3.4(c)(i);
“Vulnerability”	a weakness which allows an attacker to reduce a system's information assurance;
“Vulnerability Management”	the function responsible for the identification and possible reduction or elimination of any weakness that could be exploited by a Threat;
“Vulnerability Resolution Plan”	a plan of actions agreed with the Authority to investigate, diagnose, resolve, and prevent future occurrences of a security vulnerability.

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

1. INTRODUCTION**1.1 Service Performance Management objectives and fundamental principles**

- (a) The objectives of this Annex 3 (*TS Performance Levels*) are:
 - (i) to ensure that the Transitional Services meet the TS Performance Levels and other requirements of this Schedule 34 and of the Authority to enable consistently high-quality services;
 - (ii) to provide a mechanism whereby the TS Performance Levels can be modified and calibrated over the TS Term in response to the changing requirements of the Authority and the Service Recipients; and
 - (iii) to incentivise the Supplier to:
 - (A) meet the TS Performance Levels; and
 - (B) promptly rectify any failure to meet the TS Performance Levels.
- (b) This section sets out the fundamental Service Performance Management principles:
 - (i) The availability of TS Service Lines shall be managed to enable the Authority and all the Service Recipients and End Users to discharge their functions and duties.
 - (ii) TS Service Credits, TS Performance Levels and TS Service Credit Point measures and mechanisms shall be as set out in this Annex 3 (*TS Performance Levels*) subject to such detailed additions and amendments as the Authority determines necessary to make them operate efficiently and effectively; to the extent that a mechanism or measure currently does not operate clearly or logically, the Authority shall be entitled to determine how it should operate based on the underlying principles behind the given mechanism or measure or (if this is not capable of determination) as the Authority shall determine acting reasonably.
 - (iii) TS Service Credits shall be subject to the cap set out in [Paragraph 6] of Annex 15 (*TS Charges and Invoicing*) to this Schedule 34.
 - (iv) TS Service Credits shall continue to apply during remediation, pursuant to a Recovery Plan, a Rectification Plan or any of the measures identified in this Annex 3.

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (v) The Service Measurement Period for each TS Performance Level shall, unless otherwise provided in Appendix A, be one (1) calendar month during the TS Term.
- (vi) The TS Performance Levels and method of measuring all TS Performance Levels shall be as described in the relevant table for each TS Performance Level set out in Appendix A to this Annex 3.
- (vii) To the extent that any conflict or inconsistency exists between the provisions of this Annex 3 (*TS Performance Levels*) and the Service Performance Management principles set out in this Paragraph (b):
 - (A) the Supplier shall highlight this to the Authority; and
 - (B) Paragraph (ii) shall apply; or
 - (C) at the sole discretion of the Authority, the Supplier shall follow the Change Control Procedure.

1.2 Performance Level Principles

- (a) TS Performance Levels describe the specific performance characteristics and requirements of the Transitional Services.
- (b) The principles governing the establishment and review of TS Performance Levels and the application of TS Service Credits during the TS Term shall be as follows:
 - (i) all TS Performance Levels shall be relevant and important to the effective delivery of the Authority's business; and
 - (ii) all TS Performance Levels shall be measurable.
- (c) The TS Performance Levels are focussed on the Authority, reflect the needs of the Authority and represent the service quality that is required by the Authority, the Service Recipients and End Users.
- (d) The Supplier shall work collaboratively with relevant Other Suppliers and Replacement Suppliers to deliver the Transitional Services and TS Performance Levels.
- (e) The Supplier shall be open, transparent and honest with the Authority about the levels of performance and service quality that the Supplier is achieving.
- (f) The Supplier shall deliver the Transitional Services such that the performance proposed for the Transitional Services or any component thereof, and captured in the documentation for the Transitional Services,

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

enable the Transitional Services to be delivered to the TS Performance Levels specified in this Annex 3 (*TS Performance Levels*).

1.3 Changes to the TS Performance Levels

- (a) The Supplier shall, when directed by the Authority, conduct a review of the TS Performance Levels and the Maximum TS Service Credit Points to Reach Cap every six (6) months. As a result of the review of the TS Performance Levels, in response to changing Authority business demand or Supplier performance, the Authority may wish to vary the TS Performance Levels. As a result of the review of the Maximum TS Service Credit Points to Reach Cap, in response to reductions in the TS Charges and/or Sites, the Authority may wish to vary the Maximum TS Service Credit Points to Reach Cap so that TS Service Credits continue to be an effective remedy for the remaining Transitional Services. The Supplier shall not unreasonably withhold agreement to such variations or changes and this shall be managed through the Change Control Procedure.
- (b) The Supplier may, when directed by the Authority, conduct additional reviews of the TS Performance Levels to those set out at Paragraph (a), at any time. The Supplier shall co-operate with any additional review to that set out in Paragraph (a) of the TS Performance Levels. The Supplier shall not unreasonably withhold agreement to the introduction of new, or amendment of existing, TS Performance Levels that are applied to the Transitional Services and this shall be managed through the Change Control Procedure.
- (c) Where changes are introduced in accordance with this Paragraph 1.3, they shall be recorded in the relevant section of this Annex 3 (*TS Performance Levels*) and relevant documentation shall be updated accordingly.

1.4 Management and Measurement of TS Performance Levels

- (a) The Supplier shall measure and manage TS Performance Levels. The Supplier shall provide TS Management Information and TS Service Credit information to the Authority in accordance with this Annex 3 (*TS Performance Levels*). The TS Management Information shall provide details of, but not be limited to:
 - (i) TS Service Availability of the Transitional Services;
 - (ii) TS Incident management and resolution;
 - (iii) Security Incident Management;
 - (iv) Request fulfilment, including the activities and tasks that make up a TS Service Request;

ANNEX 3 (TS PERFORMANCE LEVELS) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (v) other TS Performance Level performance in the provision of the Transitional Services; and
 - (vi) performance against other obligations in this Schedule 34.
- (b) TS Service Level Targets and TS KPI Targets are set and measured for individual TS Performance Levels. Any TS Service Level Target failure shall be a failure to achieve that TS Service Level and any TS KPI Target failure shall be a failure to achieve that TS KPI.

1.5 Application of this Annex 3 (TS Performance Levels)

- (a) The provisions in this Annex 3 (*TS Performance Levels*) shall apply in their entirety from the Transitional Services Commencement Date.

1.6 Credit Regime Principles

- (a) The Authority has, in consultation with the Supplier, defined a TS Service Credit Regime which is applicable to the Supplier and which compensates the Authority for poor performance and continuing or repeated poor performance.
- (b) The Supplier shall be liable for remedies in the form of TS Service Credits where the Transitional Services fail to meet the TS Service Level Targets set out in this Annex 3 (*TS Performance Levels*).
- (c) TS Service Level Targets attract TS Service Credits.
- (d) Subject to Paragraph 6.6, TS KPIs do not attract TS Service Credits.

2. TS SERVICE LEVEL FRAMEWORK

2.1 TS Service Levels

- (a) The Supplier shall ensure that the Transitional Services are made available and supported. Appendix A to this Annex 3 (*TS Performance Levels*) sets out the applicable TS Service Levels and TS Key Performance Indicators.

2.2 TS Service Availability and Support Availability

- (a) The Supplier shall collaborate with relevant Replacement Suppliers and Other Suppliers in seeking to ensure that the Transitional Services are made available and supported.
- (b) For the purposes of this Schedule 34, "**TS Service Availability**" means the extent to which the Transitional Services are ordinarily accessible to, usable by, performing for and responding to the Authority and all the Service Recipients, and End Users in the discharge of their functions

ANNEX 3 (TS PERFORMANCE LEVELS) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

and duties but excluding agreed maintenance down-time. The method of measuring TS Service Availability for the TS Service Levels is set out in Appendix A.

- (c) TS Service Availability shall be measured, and TS Service Credit Points shall be calculated, in accordance with the relevant TS Service Availability SLA tables set out in Appendix A.
- (d) Severity 3 and Severity 4 Incidents (as defined in Paragraph 3.4(a) below) shall not constitute a TS Service Line being classified as Unavailable.
- (e) The service and support hours applicable to the Transitional Services are set out in Table 1, below.

TS Service Line(s)	TS Service Availability Hours	Service Hours
PSN WAN Services (Private VPN Service)	24 x 7: 24 hours, every day	24 x 7: 24 hours, every day
[REDACTED]	Monday to Friday 08:00 to 18:00 excluding English and Welsh bank holidays	Monday to Friday 08:00 to 18:00 excluding English and Welsh bank holidays
Direct Internet Access (DIA)	24 x 7: 24 hours, every day	24 x 7: 24 hours, every day
Enterprise Broadband	24 x 7: 24 hours, every day	24 x 7: 24 hours, every day
Mobile Broadband	Monday to Friday 08:00 to 18:00 excluding English and Welsh bank holidays	Monday to Friday 08:00 to 18:00 excluding English and Welsh bank holidays
TS Gateway	24 x 7: 24 hours, every day	24 x 7: 24 hours, every day

Table 1 TS Service Availability Hours and Service Hours

3. TS PERFORMANCE LEVEL TARGETS AND MEASUREMENT

3.1 TS Service Level Targets and Thresholds for TS Service Availability

- (a) TS Service Availability, TS Service Level Targets and TS Service Level Thresholds for the Transitional Services shall be those detailed within Appendix A to this Annex 3 (*TS Performance Levels*).
- (b) The TS Service Level Targets are the required TS Service Availability and performance levels below which TS Service Credits are applied as per Paragraph 4 of this Annex 3 (*TS Performance Levels*) for the Transitional Services or any component thereof.

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (c) The TS Service Level Thresholds are the trigger points at which the measures in Paragraph 6 shall apply.

3.2 TS Service Availability Measurement

- (a) The methods and Service Measurement Period(s) for the measurement of TS Service Availability for the Transitional Services shall be as set out in Appendix A.
- (b) Unavailability of a TS Service Line shall be deemed to have occurred when the state described in Paragraph 2.2(b) is not achieved.
- (a) Unavailability commences at the point an applicable auto generated event is logged, or a relevant TS Incident is opened, whichever is the earlier.
- (b) Unavailability continues until TS Service Availability is restored.
- (c) For the purpose of TS Service Availability measurement, where the Transitional Services fail to meet the relevant TS Service Level Threshold, they shall be deemed Unavailable for the duration of such failure.

3.3 TS Service Availability Calculation

- (a) TS Service Availability achieved shall be calculated for the Transitional Services in each Service Measurement Period as a percentage (rounded to two decimal places) using the applicable formula set out in the relevant TS Service Availability SLA tables in Appendix A.

3.4 TS Incident Resolution

- (a) TS Incident Severity and Priority Definitions
 - (i) TS Incidents shall be assigned Severity based on the definitions as set out in Table 2 below.
 - (ii) The Supplier shall ordinarily assign the Incident Resolution Priority equal to the Incident's Severity.
 - (iii) The Authority reserves the right to reassign an Incident Resolution Priority for any TS Incident different from that assigned by the Supplier, in which case the Supplier shall accept such Incident Resolution Priority and Incident Severity.

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Severity (Impact)	Definition
1 (Extensive)	Failure or Unavailability, or reduction in performance or loss of functionality of a TS Service Line, that prevents a group from completing its work with critical business impact.
2 (Significant)	Failure, or Unavailability, or reduction in performance or loss of functionality of a TS Service Line, that prevents a group from completing its work with significant business impact.
3 (Moderate)	Failure or Unavailability, or reduction in performance or loss of functionality of a TS Service Line, that prevents a group from completing its work, but without significant business impact; OR a single End User is impacted by Unavailability, loss of functionality or a reduction in performance of a TS Service Line.
4 (Minor)	Any other TS Incident that is none of the above and has no impact from an End User perspective but requires management.

Table 2 TS Incident Severity Levels and Definitions

- (b) TS Service Level Targets for Incident Resolution
 - (i) The Supplier shall provide Incident Management in respect of the Transitional Services.
 - (ii) The Supplier shall work with Other Suppliers and Replacement Suppliers to support the provision of end to end TS Service Incident Management, in accordance with the Incident Resolution TS Service Level Targets as set out in Appendix A.
- (c) The Authority may by giving notice to the Supplier in writing from time to time within the Authority Site List:
 - (i) designate an Authority Site that is vital to the delivery of the Authority's and/or Service Recipient's mission-critical activities as a "**VIP Site**"; and
 - (ii) de-classify an Authority Site so that it is no longer designated as a VIP Site,

provided that the total number of VIP Sites at any time does not exceed [REDACTED].
- (d) Subject to Paragraph (e), the Authority may require the Supplier to apply a higher priority to, or to use best endeavours to, achieve urgent

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

resolution of any TS Incident relating to a VIP Site, and the Supplier shall comply with this requirement.

- (e) For the avoidance of doubt, Paragraph (d) shall not affect the TS Incident Severity level for the purposes of measuring the performance against any relevant TS Service Level.
- (f) TS Incident Exclusions
 - (i) TS Incidents shall be excluded from the service level calculations where they can be shown to be as a result of faults with services other than the Transitional Service(s).
 - (ii) TS Incidents closed with the following reasons will be excluded from TS Service Level reporting:
 - Supplier Not at Fault;
 - Force Majeure including cable breaks;
 - No Fault Found;
 - Authority not responded after 3 attempts;
 - Not an Incident;
 - UPS Related;
 - Local Power Issue;
 - Non Service infrastructure/components;
 - Duplicate Incidents;
 - Incident resolved by user;
 - Training;
 - Approved Planned Maintenance Work;
 - any other closure reason reasonably agreed with the Authority and documented in writing between the Parties;
 - Cleared by Authority;
 - Environmental;
 - No Contact;
 - Order required;
 - Raised in Error; or
 - Related to Decom Activity.
- (g) On Hold Time
 - (i) Incident Resolution Time for a TS Incident is the time from when the TS Incident is reported to the Supplier to resolution time, minus any on-hold time. Circumstances when an Incident can be on-hold are:
 - Awaiting End User response;
 - Awaiting Minimum Data Set ("MDS");

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- Waiting for Equipment and Power Checks;
- Awaiting Change - Incident linked to an on-going Change, on-hold pending completion of Change;
- Awaiting Other Supplier;
- Awaiting Other Resolver Group
- Awaiting scheduled Site visit, where agreed with the End User;
- Unable to gain access to Site;
- Monitoring of services once a fix has been implemented; or
- Any other circumstance reasonably agreed with the Authority and documented in writing between the Parties.

(ii) Security Incident Severity

Security Incidents shall be assigned a Severity by the Supplier using the definitions set out in Table 3 as guidance, unless otherwise agreed with the Authority.

Severity (Impact)	Definition
1 (Critical)	A Security Incident that causes, or may cause, the degradation of vital services for a large number of End Users and involves a serious breach of network security and/or affects mission critical equipment or services and/or damage public confidence in the Government. Or A Security Incident that is, or is suspected to be, a concerted, repeating, targeted, effort causing harm to confidentiality, integrity or availability of ICT systems or data. Or Loss of an information-bearing asset where it has not been verified that the data is in a secure state.
2 (Significant)	A Security Incident that is not Critical and which impacts, or may impact, a smaller group of End Users and disrupts non-essential services and/or breaches network security policy and/or affects the reputation of Government bodies and services. Or

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Severity (Impact)	Definition
	A Security Incident that is, or is suspected to be, a targeted attack attempting to cause harm to confidentiality, integrity or availability of ICT systems or data.
3 (Minor)	A Security Incident that is not Critical or Significant and does not typically impact IT services and includes instances such as unsuccessful denial-of-service attacks or the majority of network monitoring alerts. Or A Security Incident that is likely to be non-targeted. Or Loss of an information-bearing asset where the data is in a secure state. Or Instances where activity or behaviour is recognised as suspicious but lack supporting evidence.
4 (Negligible)	A Security Incident that is not Critical, Significant or Minor and which is in general considered to be part of normal IT support operations. These Incidents would include receipt of an isolated spam or anti-virus alert, minor computer hardware failure, loss of network connectivity to a peripheral device or loss of access to an external, non-essential service.

Table 3 Security Incident Severity Definitions

- (iii) The Authority reserves the right to determine a Security Incident Severity for any Security Incident different from that initially assigned.
- (iv) The Supplier shall accept and work to the Security Incident Severity.
- (v) The Supplier shall provide Security Incident Management in accordance with the Security Incident Severity definitions set out in Table 3 below.
- (vi) The Supplier shall work with relevant Other Suppliers and Replacement Suppliers for the provision of Security Incident

ANNEX 3 (TS PERFORMANCE LEVELS) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Management, as set out in the Transitional Services Description, in accordance with TS SLA 10 (Security Incident Response) and TS SLA 11 (Security Incident Resolution / Provision of Security Incident Resolution Plan) tables set out in Appendix A.

3.5 Vulnerability Management

- (a) The Supplier shall provide Vulnerability Management, as set out in Annex 5 (*TS Security Management*) to Schedule 34. For each relevant Vulnerability, the Supplier shall specify within the Vulnerability Resolution Plan the timescale for implementation of the resolution to the Vulnerability ("**the Vulnerability Patch Deployment Time**") in accordance with the timescales set out in Appendix B. The Vulnerability Patch Deployment Time shall be measured from the point of identification or notification of the Vulnerability.

3.6 TS Service Request Management

- (a) The Supplier shall provide end to end management of the fulfilment of TS Service Requests and shall work with Other Suppliers (where applicable) to fulfil TS Service Requests.
- (b) Each individual TS Service Request for catalogue services shall be individually described within the Supplier's TS Product and Service Catalogue and shall be delivered in accordance with the individual performance measures assigned to that TS Service Request within the Supplier's TS Product and Service Catalogue.
- (c) Where there is no fulfilment time stated in the TS Product and Service Catalogue, the fulfilment time shall be agreed between the Authority and the Supplier on a case by case basis. The Authority may identify key TS Service Requests as Measured Catalogue Items, in which event these will be set out in Appendix A to this Annex 3 (*TS Performance Levels*).
- (d) The Authority shall be entitled to add Measured Catalogue Items at its discretion and without amendment to the TS Charges provided that there shall not be more than 20 Measured Catalogue Items at any one time. This shall include any Measured Catalogue Items that have been promoted to TS Service Levels Targets, in accordance with Paragraph (e).
- (e) The Authority reserves the right to promote certain TS Service Requests to TS Service Level Targets in their own right and assign TS Service Credits individually to these.

3.7 TS Project Requests

- (a) The Supplier shall provide end to end management of the fulfilment of TS Project Requests as set out in the Transitional Services Description.

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) The Supplier shall work with Other Suppliers to provide to the Authority a TS Project Proposal in response to a TS Project Request within the times set out in TS SLA 12 (TS Project Requests) for Approval, subject to the volume of TS Project Requests at any given time in which case the Authority and Supplier shall act reasonably and negotiate in good faith as to an alternative response time.
- (c) In circumstances where the scope or scale of a TS Project Request is sufficiently large or complex (as reasonably determined by the Authority or advised by the Supplier) then the Authority and the Supplier shall agree an alternative response time.
- (d) The Supplier shall report on the performance of the Supplier in achieving the response times (howsoever determined).

3.8 TS Key Performance Indicators (TS KPIs)

- (a) The Supplier shall deliver the Transitional Services and components thereof to meet the TS KPIs set out in Appendix A to this Annex 3 (*TS Performance Levels*).

4. TS SERVICE CREDITS REGIME**4.1 TS Service Availability – TS Service Credit Points Accrual**

- (a) TS Service Credit Points shall be applied in respect of each TS Service Availability TS Service Level Target breach in a Service Measurement Period.
- (b) For each TS Service Availability TS Service Level Target breach, the TS Service Credit Points in each Service Measurement Period for the relevant Transitional Services shall be calculated in accordance with the relevant TS Service Availability TS SLA tables within Appendix A.
- (c) Where the TS Service Availability TS Service Level Thresholds set out in Appendix A are exceeded, Paragraph 6.5 of this Annex 3 (*TS Performance Levels*) shall apply.
- (d) The Supplier shall work with the Authority to conduct TS Incident root cause analysis.
- (e) In respect of and during the delivery of a TS Project, where a Service Commencement Date for a Project occurs part way through a Service Measurement Period, the measurement of TS Service Availability in

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

respect of that service shall commence from the beginning of the subsequent Service Measurement Period.

4.2 TS Incident Resolution - TS Service Credit Points Accrual

- (a) Incident Resolution TS Service Credit Points can be incurred or recovered by exceeding or failing to achieve the TS Service Level Targets for Incident Resolution.
- (b) At the end of each Service Measurement Period, the Supplier shall calculate the number of minutes taken to resolve each TS Incident.
- (c) For Severity 1 and Severity 2 Incidents and in accordance with TS SLA 6 (Severity Level 1 TS Incident Resolution) and SLA 7 (Severity Level 2 TS Incident Resolution) tables set out in Appendix A, the number of minutes taken to resolve each Severity 1 and Severity 2 TS Incident shall be calculated, and the extent to which the Incident Resolution Time exceeds the relevant Incident Resolution TS Service Level Target shall be the basis on which TS Service Credit Points shall be awarded.
- (d) For the avoidance of doubt, every single Severity 1 and Severity 2 TS Incident which is not resolved within the relevant Incident Resolution TS Service Level Target attracts TS Service Credit Points separately.
- (e) For Severity 3 TS Incidents and in accordance with TS SLA 8 (Severity Level 3 Incident Resolution) table set out in Appendix A:
 - (i) the total number of Severity 3 TS Incidents that are resolved within the TS Service Level Target shall be calculated and expressed as a percentage of the total number of Severity 3 Incidents resolved; and
 - (ii) the calculated percentage shall be the basis on which TS Service Credit Points shall be awarded.
- (f) Where the Incident Resolution TS Service Level Thresholds set out in Appendix A are exceeded, Paragraph 6.5 of this Annex 3 (*TS Performance Levels*) shall apply.
- (a) Severity 4 TS Incidents shall not attract TS Service Credit Points.

4.3 Security Incident – TS Service Credit Points Accrual

- (a) Security Incident TS Service Credit Points are incurred by failing to achieve the TS Service Level Targets for any single Security Incident in accordance with TS SLA 10 (Security Incident Response) and TS SLA 11 (Security Incident Resolution / Provision of Security Incident Resolution Plan) tables set out in Appendix A.

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) Incident Resolution Times for any single Security Incident shall exclude any resolution time in relation to which all of the following apply:
 - (i) the Security Incident's resolution was delayed by a failure of a Replacement Supplier to report and/or assist as required under its agreement with the Authority, or with the Authority, in the resolution of the Incident; and
 - (ii) the Supplier seeking to rely on this exclusion has performed all of its applicable obligations as they relate to the Incident and used all reasonable endeavours to resolve the Incident and mitigate its impact.
- (c) Where the TS Service Level Thresholds set out in tables TS SLA 10 (Security Incident Response) and TS SLA 11 (Security Incident Resolution / Provision of Security Incident Resolution Plan) of Appendix A are exceeded, Paragraph 7 of this Annex 3 (*TS Performance Levels*) shall apply.

4.4 Request fulfilment – TS Service Credits

- (a) Request fulfilment TS Service Credits (where applicable) shall apply to the Supplier as set out in Appendix A to this Annex 3 (*TS Performance Levels*).

4.5 Management of TS Service Credits

- (a) The Supplier shall report on all the TS Performance Levels and shall measure and monitor performance of the Transitional Services against the TS Service Level Targets and TS KPI Targets and report these to the Authority in accordance with Paragraph 5 below.
- (b) The Supplier shall work with the Authority to calculate the total TS Service Credit Points accrued by the Supplier for all TS Service Levels that have associated TS Service Credits.
- (c) The Supplier acknowledges that the decision of the Authority on the total number of TS Service Credit Points shall be final and binding.
- (d) Where the Supplier's performance exceeds the applicable TS Service Level Targets in a Service Measurement Period, which results in negative TS Service Credit Points accruing, such negative TS Service Credit Points shall be used solely to offset against any positive TS Service Credit Points incurred by failing to achieve the TS Service Level Targets. Negative TS Service Credit Points may be accrued by the Supplier over the TS Term.
- (e) The total TS Service Credit Points accrued by the Supplier in the Service Measurement Period will be multiplied by the monetary value for each

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

TS Service Credit Point by using the formula set out in [Paragraph 6.2] of Annex 15 (*TS Charges and Invoicing*) to this Schedule 34. References in [Paragraph 6.2] of Annex 15 (*TS Charges and Invoicing*) to this Schedule 34 to "Service Period" should be read to mean "Service Measurement Period" as defined by this Annex 3 (*TS Performance Levels*).

- (f) The monetary value of the TS Service Credit Points will be credited by the Supplier to the Authority in the form of TS Service Credits in accordance with [Paragraph 6] of Annex 15 (*TS Charges and Invoicing*) to this Schedule 34.
- (g) For each Service Measurement Period the total financial value of TS Service Credits for the Supplier shall not exceed the TS Service Credit Cap.

5. TS SERVICE LEVELS REPORTING AND MANAGEMENT INFORMATION**5.1 Supplier Responsibilities**

- (a) In accordance with the Transitional Services Description, the Supplier shall report on the performance of the Transitional Services against the TS Service Levels and TS KPIs specified herein and shall provide the Authority with the relevant information pertaining to the Transitional Services, or any components thereof, for each Service Measurement Period.
- (b) The Supplier shall also include in the report a management summary of TS Service Level and TS KPI performance.

5.2 TS Management Information Content

- (a) The Supplier shall provide TS Management Information for each Service Measurement Period, and in accordance with the Transitional Services Description and this Annex 3 (*TS Performance Levels*). This TS Management Information shall include, but not be limited to the achievement or non-achievement of TS Service Levels and TS KPIs for Transitional Services and the accumulation of TS Service Credit Points.
- (b) The TS Management Information shall include details of, but not be limited to:
 - (i) TS Service Availability of Transitional Services;
 - (ii) TS Incident management and resolution;
 - (iii) Security Incident management;
 - (iv) Request fulfilment;

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (v) other TS Performance Level performance in the provision of Transitional Services;
- (vi) performance against other obligations in this Schedule 34; and
- (vii) ITSM practices that have a reliance or dependency upon the Authority, Replacement Suppliers or Other Suppliers.

**6. MANAGEMENT AND ESCALATION OF TS SERVICE LEVEL TARGETS
AND TS SERVICE LEVEL THRESHOLD FAILURES**

6.1 Introduction

- (a) The procedures set out in this Paragraph 6 are intended to enable the Supplier to manage service issues arising from failure to achieve the TS Service Level Targets, TS Service Level Thresholds and TS KPI Targets set out in this Annex 3 (*TS Performance Levels*).
- (b) The TS Service Credit provisions of this Annex 3 (*TS Performance Levels*) shall continue to apply throughout the Escalation Process.
- (c) The Supplier shall proactively resolve outstanding issues relating to failures to achieve TS Service Level Targets, TS Service Level Thresholds and TS KPI Targets, in addition to the procedures set out in this Paragraph 6, assess the need for further remedial action to prevent recurrence of such failures.
- (d) Where such further remedial action is required, the Supplier shall follow the Rectification Plan Process set out in Clause 25. The scope and format of all Rectification Plans shall be defined and documented by the Authority in the TS Service Level Management Policies, Processes and Procedures, as set out in the Transitional Services Description.

6.2 Repeated TS Service Availability TS Service Level Target failures

- (a) Where the TS Service Availability of a TS Service Line is below its TS Service Level Target but above the TS Service Level Threshold for two (2) Service Measurement Periods in a four (4) month rolling period, the Supplier working with Other Suppliers (where applicable) shall highlight this and provide an action plan to mitigate any continuing trend to the Authority within five (5) Working Days of the second TS Service Level Target breach.
- (b) Where the TS Service Availability of a Transitional Services Line is below its TS Service Level Target but above the TS Service Level Threshold on three (3) or more instances in a four (4) month rolling period, the following shall be required:
 - (i) the Supplier shall produce a Recovery Plan and submit the Recovery Plan to the Authority within five (5) Working Days of the third TS Service Level Target failure;

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (ii) the Recovery Plan shall specify the remedial actions and activities to be undertaken and the recovery period;
 - (iii) the Authority shall review the Recovery Plan (including timescales), and decide whether to Approve the Recovery Plan;
 - (iv) following Approval, the Supplier shall commence implementation of the Recovery Plan within five (5) Working Days; and
 - (v) the implementation of the Recovery Plan shall be reviewed on a weekly basis by the Parties, until the Recovery Plan is completed.
- (c) If the TS Service Availability of the relevant TS Service Line(s) on completion of the Recovery Plan progressed under Paragraph (b) fails to achieve the relevant TS Service Availability TS Service Level Target due to a related TS Incident in the following Service Measurement Period, then this shall constitute a Material TS Service Level Failure and the Supplier shall follow the Rectification Plan Process in Clause 25.
- (d) If the TS Service Availability of the relevant TS Service Line(s), on completion of a Rectification Plan progressed under Paragraph (c), achieves the relevant TS Service Level Target and then consequently fails to achieve the same TS Service Level Target in any of the three (3) subsequent Service Measurement Periods, due to a related TS Incident, then this shall constitute a Critical TS Service Failure.

6.3 Multiple Severity 1 TS Incidents in a Service Measurement Period

- (a) Where there are any three (3) individual Severity 1 TS Incidents for a TS Service Line comprising part of the Transitional Services with a similar root cause within a Service Measurement Period, an Exception Report shall be required. The Supplier shall submit an Exception Report to the Authority within five (5) Working Days of the third Severity 1 TS Incident.
- (b) In the event of a fourth Severity 1 Incident for a TS Service Line with a similar root cause within the same Service Measurement Period, this shall constitute a Material TS Service Level Failure and the Supplier shall follow the Rectification Plan Process in Clause 25.
- (c) If the same TS Service Line, on completion of a Rectification Plan progressed under Paragraph (b), has more than one (1) related Severity 1 TS Incident in the next Service Measurement Period, then this shall constitute a Critical TS Service Failure.

6.4 Other repeated TS Service Level Target Breaches

- (a) This Paragraph 6.4 applies to repeated breaches of TS Service Level Targets other than the TS Service Availability of a TS Service Line and multiple Severity 1 TS Incidents.

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (b) Where a TS Service Level Target is not achieved in any three (3) Service Measurement Periods out of six (6) Service Measurement Periods on a rolling six (6) month basis, the following shall be required:
 - (i) the Supplier shall produce a Recovery Plan and submit the Recovery Plan to the Authority within five (5) Working Days of the third TS Service Level Target failure;
 - (ii) the Recovery Plan shall specify the remedial actions and activities to be undertaken and the recovery period;
 - (iii) the Authority shall review the Recovery Plan (including timescales), and decide whether to Approve the Recovery Plan;
 - (iv) following Approval, the Supplier shall commence implementation of the Recovery Plan within five(5) Working Days; and
 - (v) the implementation of the Recovery Plan shall be reviewed on a weekly basis by the Parties, until the Recovery Plan is completed.
- (c) If a TS Service Level Target is not achieved in any four (4) Service Measurement Periods out of out of six (6) Service Measurement Periods on a rolling six (6) month basis, the Authority shall determine whether a Rectification Plan is required. If the Authority deems that a Rectification Plan is required, then the Supplier shall follow the Rectification Plan Process in Clause 25.
- (d) If the TS Service Level achievement on completion of a Rectification Plan progressed under Paragraph (c) remains below the relevant TS Service Level Target, due to a related TS Incident or TS Incidents, in the following Service Measurement Period, then this shall constitute a Critical TS Service Failure.

6.5 TS Service Level Threshold Breach

- (a) Where the TS Service Availability at a Site, Incident Resolution or performance of a Service is below its TS Service Level Threshold for a Service Measurement Period, the following shall be required:
 - (i) the Supplier shall produce a Recovery Plan and submit the Recovery Plan to the Authority within five (5) Working Days of the TS Service Level Threshold breach;
 - (ii) the Recovery Plan shall specify the remedial actions and activities to be undertaken. The plan shall also specify the proposed recovery period which shall be as soon as possible and, in any event, no less than within the following Service Measurement Period, following Approval;

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (iii) the Authority shall review the Recovery Plan (including timescales) and decide whether to Approve the Recovery Plan;
 - (iv) following Approval, the Supplier shall commence implementation of the Approved Recovery Plan within two (2) Working Days and all actions thereunder shall be implemented no later than the end of the next Service Measurement Period; and
 - (v) the implementation of the Recovery Plan shall be reviewed on a weekly basis by the Authority and Supplier until the Recovery Plan is completed.
- (b) If, on completion of a Recovery Plan progressed under Paragraph (a), the TS Service Availability at the relevant Site, Incident Resolution or performance of the Service remains below its TS Service Level Threshold in a second consecutive Service Measurement Period, then this shall constitute a Material TS Service Level Failure and the Supplier shall follow the Rectification Plan Process in Clause 25.
- (c) If the TS Service Availability at the relevant Site, Incident Resolution or performance of the Service, on completion of the Rectification Plan, achieves the TS Service Level Target and then consequently fails to achieve the TS Service Level Target due to a related TS Incident in any of the three (3) subsequent Service Measurement Periods then this shall constitute a Critical TS Service Failure.

6.6 Repeated TS KPI Breaches

- (a) Where a TS KPI Target is not achieved in any three (3) Service Measurement Periods out of six (6) Service Measurement Periods on a rolling six (6) month basis, the Supplier working with Other Suppliers (where applicable) shall highlight this to the Authority within five (5) Working Days of the third instance of TS KPI Target non-achievement.
- (b) Following notification of the TS KPI non-achievement under Paragraph (a), the Authority shall determine whether a Recovery Plan is required. If the Authority deems that a Recovery Plan is required, then the Authority shall notify the Supplier and:
 - (i) the Supplier shall produce a Recovery Plan and submit the Recovery Plan to the Authority within nine (9) Working Days of notification from the Authority;
 - (ii) the Recovery Plan shall specify the remedial actions and activities to be undertaken and the recovery period;
 - (iii) the Authority shall review the Recovery Plan (including timescales), and decide whether to Approve the Recovery Plan;

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- (iv) following Approval, the Supplier shall commence implementation of the Approved Recovery Plan within six (6) Working Days; and
 - (v) the implementation of the Recovery Plan shall be reviewed on a weekly basis by the Authority and the Supplier until the Recovery Plan is completed.
- (c) If the TS KPI achievement on completion of the Recovery Plan remains below the TS KPI Target in the following Service Measurement Period, then the Authority reserves the right to promote the TS KPI to be a TS Service Level Target.
- (d) The Authority reserves the right, on a Quarterly basis, to promote any TS KPI that has not been consistently achieved to a TS Service Level Target following consultation and agreement with the Supplier. The Supplier shall not unreasonably withhold agreement to promote any TS KPI that has not been consistently achieved to a TS Service Level Target.
- (e) Any TS KPI which has been promoted to a TS Service Level Target shall be measured and reported on as a TS Service Level Target, and the associated TS Service Credit Points applied, within two (2) Service Measurement Periods.
- (f) Any TS KPI which has been promoted to a TS Service Level Target in accordance with Paragraph (d) of this Annex 3 (*TS Performance Levels*), shall be measured and reported on as a TS Service Level Target until the TS Service Level Target has been achieved for four (4) consecutive Service Measurement Periods, after which the TS Service Level Target shall revert to a TS KPI.
- (g) Paragraph 6.6(f) of this Annex 3 (*TS Performance Levels*) shall not apply where the Authority has promoted a TS KPI to a TS Service Level Target in accordance with Paragraph 1.3 of this Annex 3 (*TS Performance Levels*).

6.7 Severity 2 Incident TS Service Level Target Breaches

- (a) Subject to Paragraph (c), any Severity 2 TS Incident not resolved by the relevant Incident Resolution TS Service Level Target shall be automatically uplifted to a Severity 1 TS Incident for the purposes of governance, management and Management Information until the TS Incident is closed unless otherwise agreed with the Authority.
- (b) The number of Severity 2 TS Incidents promoted to Severity 1, as a result of Incident Resolution TS Service Level Target Failure, within the Service Measurement Period shall be reported by the Supplier.
- (c) For purposes of Incident Resolution TS Service Level Targets and TS Service Credit Point accrual, any Severity 2 TS Incident that has been

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

promoted to a Severity 1, as a result of Incident Resolution TS Service Level Failure, shall continue to be treated as a Severity 2 TS Incident.

6.8 Critical TS Service Failures

- (a) If the level of performance by the Supplier in respect of the Transitional Services constitutes a Critical TS Service Failure under any of Paragraphs 6.2 to 6.7 of this Annex 3 (*TS Performance Levels*), the Authority shall be entitled to terminate this Contract pursuant to Clause 31.1(b) due to the occurrence of limb (a) of the definition of Supplier Termination Event (as amended by Paragraph 31.1 of Schedule 34) and/or exercise its right of partial termination pursuant to Clause 31.2(b).
- (a) Nothing in Paragraph 6 of this Annex 3 (*TS Performance Levels*) shall limit or adversely affect any rights and remedies available to the Authority.

7. IT SERVICE CONTINUITY MANAGEMENT

- 7.1 IT Service Continuity Management (ITSCM) is the restoration of the Transitional Services to the agreed RTO and RPO to support the overall Authority Business Continuity Strategy and Plans.
- 7.2 IT Service Continuity Management (ITSCM) is an obligation of the Supplier.
- 7.3 No TS Service Credits apply to ITSCM itself.
- 7.4 The determination of a “Disaster” is at the Authority’s discretion.
- 7.5 The Supplier shall work with the Other Suppliers to ensure that the Transitional Services are provided as per the ITSCM Categories defined in Table 4 with an RTO of Silver and an RPO of Bronze.

ITSCM Category	
RTO	
Platinum	No Service loss
Gold	≤ 1 hour Service loss
Silver	≤ 4 hours Service loss
Bronze	≤ 24 hours Service loss
Brass	≤ 120 hours Service loss
RPO	
Platinum	No data loss
Gold	≤ 1 hour data loss
Silver	≤ 4 hours data loss
Bronze	≤ 24 hours data loss
Brass	≤ 120 hours data loss

Table 4 ITSCM RTO and RPO Categories

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

8. SUPPLIER PERFORMANCE SCORECARD

- 8.1 The Authority may produce a template Supplier Performance Scorecard during the term of this Agreement which shall be developed and agreed with the Supplier in accordance with the Change Control Procedure.

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

APPENDIX A – TS SERVICE LEVELS AND TS KPIs

Introduction

This Appendix sets out the TS Service Levels and TS KPIs which shall be used to measure the performance of the Transitional Services by the Supplier and (where relevant) their associated TS Service Credits.

The TS Service Levels and TS KPIs set out in this Appendix shall be measured and reported on by the Supplier.

Unless otherwise specified, all TS Service Levels and TS KPIs shall be applied to activities during the previous Service Measurement Period.

TS Service Level Targets

The TS Service Level Targets and TS KPI Targets shall be as set out in the Tables below.

- 1. TS Service Availability
- 2. Incident Response and Resolution
- 3. Request fulfilment
- 4. TS Key Performance Indicators (TS KPIs)

1. TS Service Availability

SLA 1 – Site Availability	
Description	The percentage Availability for each Site receiving the Transitional Services within a Service Measurement Period ('SMP').
Calculation	The actual TS Service Availability achieved shall be calculated using the following formula rounded to two decimal places: $\text{Actual TS Service Availability (\%)} = \frac{(\text{SA} - \text{SU})}{\text{SA}} \times 100$ Where: SA = Total number of available minutes within the SMP; and SU = Total number of minutes of TS Service Unavailability within the SMP, calculated as the sum of the individual occurrences of TS Service Unavailability.
Exclusions	As set out in Paragraph 3.4(f) of this Annex 3 (<i>TS Performance Levels</i>).

ANNEX 3 (TS PERFORMANCE LEVELS) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Service Measurement Period	The SMP for this service is one calendar month. The SLA measurement time shall be as per the Service Hours defined in table 1 of Paragraph 2.2(e) of this Annex 3 (<i>TS Performance Levels</i>).	
Service Resilience	Resilient/Dual Connected Site	Non-Resilient/Single Connected Site
TS Service Level Target	99.9%	99.75%
TS Service Level Threshold	98%	98%
TS Service Credit Points per TS Service Credit Increment and TS Service Line	PSN WAN Services (Private VPN Service) – 35 DIA (Resilient Pair) – 35 [REDACTED] 35	PSN WAN Services (Private VPN Service) – 35 DIA – 35 [REDACTED] 35
TS Service Credit Point Calculation	The number of TS Service Credit Points shall be calculated using the following formula: $\text{TS Service Credit Points} = (A - B) \times 1000 \times C$ Where: A = TS Service Level Target (%); B = Actual TS Service Availability (%); and C = number of points (as per the service resilience and TS Service Line as set out above) for each 0.10% below the TS Service Level Target or part thereof.	
Service Exclusions	Enterprise Broadband and Mobile Broadband are excluded from Availability Target measurements.	

SLA 2 – TS Gateway

Description	A measure of the availability percentage of the TS Gateway within a Service Measurement Period.
Calculation	The actual TS Service Availability achieved for the TS Gateway shall be calculated using the following formula to calculate actual TS Service Availability achieved (rounded down to two decimal places):

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	Actual TS Service Availability (%) = $\frac{(SA - SU)}{SMP} \times 100$ Where: SA = Total number of available minutes within the SMP; and SU = Total number of minutes of TS Service Unavailability within the SMP. TS Service Unavailability shall be calculated as the sum of the individual occurrences of TS Service Unavailability for the service. For the avoidance of doubt this SLA covers the connectivity to the Supplier Supplier's provided TS Gateway only, and where the traffic volumes are within the solution design parameters.
Exclusions	As set out in Paragraph 3.4(f) of this Annex 3 (<i>TS Performance Level(s)</i>).
Service Measurement Period	The Service Measurement Period (SMP) for this TS Service Line is one calendar month. The SLA measurement time shall be as per the TS Service Availability Hours defined in Table 1 of Paragraph 2.2(e).
TS Service Level Target	99.99%
TS Service Level Threshold	98%
TS Service Credit Points	The number of TS Service Credit Points shall be calculated using the following formula: TS Service Credit Points = $(A - B) \times 1000 \times C$ Where: A = TS Service Level Target (%); B = Actual TS Service Availability (%); and C = 200 points for each 0.10% below the TS Service Level Target or part thereof.

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

2. TS Incident Response and Resolution

SLA 6 – Severity Level 1 TS Incident Resolution	
Description	Severity Level 1 TS Incidents reported to the Supplier that are Resolved within the TS Service Level Target after being reported to the Supplier.
Calculation	For TS Service Level Targets and TS Service Level Thresholds indicated in this table as being “MTTR”, then the Supplier shall calculate the arithmetic mean of the Incident Resolution Times (Mean Time to Repair) as follows: $\text{Incident Resolution Time} = \frac{\text{Total Incident Resolution Times for same TS Service Line}}{\text{Number of Incidents for same TS Service Line}}$ Otherwise, the Incident Resolution Time shall be calculated as the actual number of minutes taken to resolve each Severity 1 TS Incident. Where an Incident Resolution Time fails or exceeds the TS Service Level Target then TS Service Credit Points shall be awarded. For the avoidance of doubt, should the Supplier be investigating alongside the Authority or third party service provider, the Supplier will retain the TS Incident and include time spent in the measurement calculation. Time during which the TS Incident was not assigned to the Supplier in the TS Incident Management System will be excluded from the calculation in accordance with Paragraph 3.4(f) of this Annex 3 (<i>TS Performance Levels</i>), except where the TS Incident has been incorrectly re-assigned to another party for resolution. Should an Incident Severity Level be increased (e.g. from Severity Level 2 to Severity Level 1) then: - the time occurring prior to the Severity Level being increased shall be discounted from the calculation set out in this TS SLA; and - the Supplier shall have the period of time applicable to a Severity Level 1 TS Incident (two or four hours, depending upon service resilience) to achieve Incident Resolution, such period of time commencing from the time at which the Severity Level is increased.

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	The time taken by the Supplier to achieve Incident Resolution of each TS Incident reported to it shall: a) commence at the time that the Incident is reported by the Authority to the Supplier; b) end at the time that the Supplier informs the Authority that they have undertaken the necessary activities to allow the Incident to be resolved; and c) re-commence (where relevant) when a TS Incident is re-assigned to the Supplier by the Authority.			
Exclusions	As set out in Paragraph 3.4(f) of this Annex 3 (<i>TS Performance Levels</i>).			
Service Measurement Period	The Service Measurement Period (SMP) for this service is one calendar month. The measurement time shall be as per the Service Hours defined in Table 1 of Paragraph 2.2(e) of this Annex 3 (<i>TS Performance Levels</i>).			
Service Resilience	Resilient/Dual Connected Site		Non-Resilient/Single Connected Site	
TS Service Level Target per TS Service Line	PSN WAN Services (Private VPN Service) - 2 Hours MTTR [REDACTED] – 4 Hours DIA (Resilient Pair) – 4 Hours		PSN WAN Services (Private VPN Service) - 4 Hours MTTR [REDACTED] – 8 Hours DIA 8 Hours	
TS Service Level Threshold per TS Service Line	PSN WAN Services (Private VPN Service) - 12 Hours MTTR [REDACTED] and DIA - 16 Hours		PSN WAN Services (Private VPN Service) - 16 Hours MTTR [REDACTED] and DIA - 24 Hours	
PSN WAN Services (Private VPN Service) and TS Gateway TS Service Credit Points	Per Incident Resolution Time	TS Service Credit Points Incurred	Per Incident Resolution Time	TS Service Credit Points Incurred
	≤ 1 hours	-25	≤ 2 hours	-25
	> 1 hours & ≤ 2 hours	0	> 2 hours & ≤ 4 hours	0
	> 2 hours & ≤ 4 hours	25	> 4 hours & ≤ 6 hours	25
	> 4 hours & ≤ 6 hours	50	> 6 hours & ≤ 8 hours	50
	> 6 hours & ≤ 8 hours	100	> 8 hours & ≤ 12 hours	100

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	> 8 hours & ≤ 10 hours	150	> 12 hours & ≤ 16 hours	150
	Per additional 2 hours or part thereof	50	Per additional 4 hours or part thereof	50
[REDACTED] TS Service Credit Points	Per Incident Resolution Time	TS Service Credit Points Incurred	Per Incident Resolution Time	TS Service Credit Points Incurred
	≤ 2 hours	-25	≤ 4 hours	-25
	> 2 hours & ≤ 4 hours	0	> 4 hours & ≤ 8 hours	0
	> 4 hours & ≤ 6 hours	25	> 8 hours & ≤ 12 hours	25
	> 6 hours & ≤ 8 hours	50	> 12 hours & ≤ 16 hours	50
	> 8 hours & ≤ 12 hours	100	> 16 hours & ≤ 20 hours	100
	> 12 hours & ≤ 16 hours	150	> 20 hours & ≤ 24 hours	150
	Per additional 4 hours or part thereof	50	Per additional 8 hours or part thereof	50
DIA TS Service Credit Points	Per Incident Resolution Time	TS Service Credit Points Incurred	Per Incident Resolution Time	TS Service Credit Points Incurred
	≤ 2.5 hours	-25	≤ 4 hours	-25
	> 2.5 hours & ≤ 5 hours	0	> 4 hours & ≤ 8 hours	0
	> 5 hours & ≤ 10 hours	25	> 8 hours & ≤ 12 hours	25
	> 10 hours & ≤ 15 hours	50	> 12 hours & ≤ 16 hours	50
	> 15 hours & ≤ 20 hours	100	> 16 hours & ≤ 20 hours	100
	> 20 hours & ≤ 25 hours	150	> 20 hours & ≤ 24 hours	150
	Per additional 10 hours or part thereof	50	Per additional 8 hours or part thereof	50

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

SLA 7 – Severity Level 2 TS Incident Resolution	
Description	Severity Level 2 TS Incidents reported to the Supplier that are resolved within four (4) hours after being reported to the Supplier.
Calculation	For TS Service Level Targets and TS Service Level Thresholds indicated in this SLA table below as being “MTTR”, then the Supplier shall calculate the arithmetic mean of the Incident Resolution Times (Mean Time to Repair) as follows: $\text{Incident Resolution Time} = \frac{\text{Total Incident Resolution Times for same TS Service Line}}{\text{Number of Incidents for same TS Service Line}}$ Otherwise, the Incident Resolution Time shall be calculated as the actual number of minutes taken to resolve each Severity 2 TS Incident. Where an Incident Resolution Time fails or exceeds the TS Service Level Target then TS Service Credit Points shall be awarded. For the avoidance of doubt, should the Supplier be investigating alongside the Authority or third party service provider, the Supplier will retain the TS Incident and include time spent in the measurement calculation. Time during which the TS Incident was not assigned to the Supplier in the TS Incident Management System should be excluded from the calculation in accordance with Paragraph 3.4(f) of this Annex 3 (TS Performance Levels), except where the TS Incident has been incorrectly re-assigned to another party for resolution. Should an Incident Severity Level be increased (e.g. from Severity Level 3 to Severity Level 2) then: a) the time occurring prior to the Severity Level being increased shall be discounted from the calculation set out in this SLA; and b) the Supplier shall have the four-hour period of time applicable to a Severity Level 2 TS Incident to achieve Incident Resolution, such period of time commencing from the time at which the Severity Level was originally assigned. Should an Incident Severity Level be decreased (e.g. from Severity Level 1 to Severity Level 2), then:

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	a) the Supplier shall have the defined period of time applicable to the decreased Severity Level as set out above to achieve Incident Resolution, such period of time commencing from the time at which the TS Incident was originally assigned. The time taken by the Supplier to achieve Incident Resolution of each TS Incident reported to it shall: a) commence at the time that the TS Incident is reported by the Authority to the Supplier; b) end at the time that the Supplier informs the Authority that they have undertaken the necessary activities to allow the TS Incident to be resolved; and c) re-commence (where relevant) when a TS Incident is re-assigned to the Supplier by the Authority.	
Exclusions	As set out in Paragraph 3.4(f) of this Annex 3 (<i>TS Performance Levels</i>).	
Service Measurement Period	The Service Measurement Period (SMP) for this service is one calendar month. The measurement time shall be as per the Service Hours defined in Table 1 of Paragraph 2.2(e) of this Annex 3 (<i>TS Performance Levels</i>).	
TS Service Level Target per TS Service Line	PSN WAN Services (Private VPN Service) and TS Gateway–MTTR (Resilient & Non-Resilient) - 4 Hours [REDACTED] – 8 Hours DIA (Resilient & Non-Resilient) 8 Hours	
TS Service Level Threshold per TS Service Line	All other TS Service Lines – 24 Hours	
PSN WAN Services (Private VPN Service) and TS Gateway TS Service Credit Points	Per Incident Resolution Time (within Service Hours)	Service Credit Points Incurred
	≤ 2 hours	-25
	> 2 hours & ≤ 4 hours	0
	> 4 hours & ≤ 6 hours	25
	> 6 hours & ≤ 8 hours	50
	> 8 hours & ≤ 12 hours	100
	> 12 hours & ≤ 16 hours	150
	Per additional 4 hours or part thereof	50

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED] & DIA TS Service Credit Points	Per Incident Resolution Time (within Service Hours)	TS Service Credit Points Incurred
	4 hours	-25
	> 4 hours & ≤ 8 hours	0
	> 8hours & ≤ 12 hours	25
	> 12 hours & ≤ 16 hours	50
	> 16 hours & ≤ 20 hours	100
	> 20 hours & ≤ 24 hours	150
	Per additional 4 hours or part thereof	50

SLA 8 - Severity Level 3 TS Incident Resolution	
Description	Severity Level 3 TS Incidents reported to the Supplier that are resolved within eight (8) hours of being reported to the Supplier.
Calculation	The total number of Severity 3 TS Incidents that are resolved within the TS Service Level Target shall be calculated and expressed as a percentage of the total number of Severity 3 TS Incidents resolved: $A / B \times 100$ Where: A = the aggregate number of Severity Level 3 TS Incidents resolved by the Supplier in 8 hours or less within the SMP (whether such Severity Level 3 TS Incidents were reported to the Supplier in that SMP or an earlier SMP). B = the aggregate number of Severity Level 3 TS Incidents reported to and resolved within the SMP (whether such Severity Level 3 Incidents were reported to the Supplier in that SMP or an earlier SMP). For the avoidance of doubt, should the Supplier be investigating alongside the Authority or third party service provider, the Supplier will retain the TS Incident and include time spent in the measurement calculation. Time during which the TS Incident was not assigned to the Supplier in the TS Incident Management System should be excluded from the calculation in accordance with Paragraph 3.4(f) of this Annex 3 (<i>TS Performance Levels</i>), except where the TS Incident has been incorrectly re-assigned to another party for resolution. Should an Incident Severity Level be increased (ie from Severity Level 4 to Severity Level 3) then:

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**Confidential
Contract for the provision of WAN ServicesSecurity Classification (Official)
Contract reference: [REDACTED]

	a) the time occurring prior to the Severity Level being increased shall be discounted from the calculation set out in this SLA; b) the Supplier shall have the one (1) working day period of time applicable to a Severity Level 3 TS Incident to achieve Incident Resolution, such period of time commencing from the time at which the Severity Level is increased; and c) should an Incident Severity Level be decreased (e.g. from Severity Level 2 to Severity Level 3), then the Supplier shall have the defined period of time applicable to the decreased Severity Level as set out above to achieve Incident Resolution, such period of time commencing from the time at which the TS Incident was originally reported. The time taken by the Supplier to achieve Incident Resolution of each TS Incident reported to it shall: a) commence at the time that the TS Incident is reported by the Authority to the Supplier; b) end at the time that the Supplier informs the Authority that they have undertaken the necessary activities to allow the TS Incident to be resolved; and c) re-commence (where relevant) when a TS Incident is re-assigned to the Supplier by the Authority.	
Exclusions	As set out in Paragraph 3.4(f) of this Annex 3 (<i>TS Performance Levels</i>).	
Service Measurement Period	The Service Measurement Period (SMP) for this service is one calendar month. The SLA measurement time shall be as per the Service Hours defined in Table 1 of Paragraph 2.2(e) of this Annex 3 (<i>TS Performance Levels</i>).	
TS Service Level Target	[REDACTED] DIA – 98% within 2 Working Days All other Service Lines - 98% within eight (8) hours.	
TS Service Level Threshold	All TS Service Lines - 93%	
TS Service Credit Points – [REDACTED] DIA &	% TS Incidents Resolved (within Service Hours)	TS Service Credit Points Incurred
	>= 98%	0
	< 98% & >= 97%	75

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

All other Service Lines	< 97% & >= 96%	150
	< 96% & >= 95%	225
	< 95% & >= 94%	300
	< 94% & >= 93%	375
	Per additional 1% below or part thereof	75

SLA 9 – Enterprise Broadband and Mobile Broadband TS Incident Resolution	
Description	All Severity Levels reported to the Supplier.
Calculation	For TS Service Level Targets and TS Service Level Thresholds indicated in this SLA table below calculated as the actual number of minutes taken to resolve each TS Incident. For the avoidance of doubt, should the Supplier be investigating alongside the Authority or third party service provider, the Supplier will retain the TS Incident and include time spent in the measurement calculation. Time during which the TS Incident was not assigned to the Supplier in the TS Incident Management System should be excluded from the calculation in accordance with Paragraph 3.4(f) of this Annex 3 (<i>TS Performance Levels</i>), except where the TS Incident has been incorrectly re-assigned to another party for resolution. The time taken by the Supplier to achieve Incident Resolution of each TS Incident reported to it shall: a) commence at the time that the TS Incident is reported by the Authority to the Supplier; b) end at the time that the Supplier informs the Authority that they have undertaken the necessary activities to allow the TS Incident to be resolved; and c) re-commence (where relevant) when a TS Incident is re-assigned to the Supplier by the Authority.
Exclusions	As set out in Paragraph 3.4(f) of this Annex 3 (<i>TS Performance Levels</i>).
Service Measurement Period	The Service Measurement Period (SMP) for this service is one calendar month. The measurement time shall be as per the Service Hours defined in Table 1 of Paragraph 2.2(e) of this Annex 3 (<i>TS Performance Levels</i>).

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**Confidential
Contract for the provision of WAN ServicesSecurity Classification (Official)
Contract reference: [REDACTED]

Device Technical Support	The Device is not sending data/responding to connection attempts, and connectivity has been ruled out as the source of the TS Incident.	98% within 2 hours from when Supplier is notified by the Authority.
TS Service Credit Points	Per Incident Resolution Time (within Service Hours)	TS Service Credit Points Incurred
	≤ 2 hours	-10
	> 2 hours & ≤ 4 hours	0
	> 4 hours & ≤ 6 hours	10
	> 6 hours & ≤ 8 hours	20
	> 8 hours & ≤ 10 hours	30
	> 10 hours & ≤ 12 hours	40
	Per additional 4 hours or part thereof	10
Device Physical Recovery/Replacement	The Device issue cannot be resolved remotely, connectivity has been ruled out as the cause, and physical recovery of the Device is needed to further investigate the cause. or The Device has a physical defect under warranty and is being recovered for replacement/repair.	99% within 24 hours from when Supplier is notified by the Authority.
TS Service Credit Points	Per Incident Resolution Time (within Service Hours)	TS Service Credit Points Incurred
	≤ 24 hours	0
	> 24 hours & ≤ 28 hours	10
	> 28 hours & ≤ 32 hours	20
	> 32 hours & ≤ 36 hours	30
	> 36 hours & ≤ 40 hours	40
	> 40 hours & ≤ 44 hours	50
	Per additional 4 hours or part thereof	10

SLA 10 – Security Incident Response

Description	Security Incidents reported to the Supplier that are responded to within target from the point at which it was reported to the Supplier.

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**Confidential
Contract for the provision of WAN ServicesSecurity Classification (Official)
Contract reference: [REDACTED]

Calculation	The time taken (within the applicable Service Hours) by the Supplier to respond to each Security Incident reported to it by the Authority. Time during which the Security Incident was not assigned to the Supplier in the TS Incident Management System will be excluded from the calculation in accordance with Paragraph 3.4(f) of this Annex 3 (<i>TS Performance Levels</i>), except where the Security Incident has been incorrectly re-assigned to another party for resolution. For the avoidance of doubt, 'response' is a human acknowledgement of the Security Incident.			
Exclusions	As set out in Paragraph 3.4(f) of this Annex 3 (<i>TS Performance Levels</i>).			
Service Measurement Period	The Service Measurement Period (SMP) for this service is one calendar month. The measurement time shall be as per the Service Hours defined in Table 1 of Paragraph 2.2(e).			
TS Service Level Target	Severity 1 – 0.5 hours Severity 2 – 1 hour Severity 3 – 4 hours Severity 4 – 8 hours			
TS Service Level Threshold	Severity 1 – >4 hours Severity 2 – >7 hours Severity 3 – >28 hours Severity 4 – >56 hours			
TS Service Credit Points	Security Incident Response Time			
	Severity 1	Severity 2	Severity 3	Severity 4
0	≤0.5 hour	≤1 hour	≤4 hours	≤8 hours
100	>0.5 hour & ≤1 hour	>1 hour & ≤2 hours	>4 hours & ≤8 hours	>8 hours & ≤16 hours
200	>1 hour & ≤1.5 hours	>2 hours & ≤3 hours	>8 hours & ≤12 hours	>16 hours & ≤24 hours
300	>1.5 hour & ≤2 hours	>3 hours & ≤4 hours	>12 hours & ≤16 hours	>24 hours & ≤32 hours
400	>2 hours & ≤2.5 hours	>4 hours & ≤5 hours	>16 hours & ≤20 hours	>32 hours & ≤40 hours
500	>2.5 hours & ≤3 hours	>5 hours & ≤6 hours	>20 hours & ≤24 hours	>40 hours & ≤48 hours

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

100	per additional 0.5 hours or part thereof	per additional 1 hours or part thereof	per additional 4 hours or part thereof	per additional 8 hours or part thereof

SLA 11 – Security Incident Resolution / Provision of Security Incident Resolution Plan	
Description	Security Incidents reported to the Supplier that are resolved or a Security Incident Resolution Plan agreed within target from the point at which it was reported to the Supplier.
Calculation	The time taken by the Supplier to resolve each Security Incident reported to it by the Authority. Time during which the Security Incident was not assigned to the Supplier in the TS Incident Management System should be excluded from the calculation in accordance with Paragraph 3.4(f) of this Annex 3 (<i>TS Performance Levels</i>), except where the Security Incident has been incorrectly re-assigned to another party for resolution.
Exclusions	As set out in Paragraph 3.4(f) of this Annex 3 (<i>TS Performance Levels</i>).
Service Measurement Period	The Service Measurement Period (SMP) for this service is one calendar month. The SLA measurement time shall be as per the Service Hours defined in Table 1 of Paragraph 2.2(e) of this Annex 3 (<i>TS Performance Levels</i>).
TS Service Level Target	Severity 1 – ≤ 1 Working Day Severity 2 – ≤ 3 Working Days Severity 3 – ≤ 5 Working Days* <i>*unless otherwise agreed with the Authority (The Authority will act reasonably in granting additional days where such time would not exceed the Authority's patching policy (https://security-guidance.service.justice.gov.uk/patch-management-guide/#patch-management-guide)).</i>
TS Service Level Threshold	Severity 1 – >7 Working Days Severity 2 – >21 Working Days Severity 3 – >35 Working Days

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

TS Service Credit Points	Security Incident Response Time (Working Days)			
	Severity 1	Severity 2	Severity 3	Severity 4
0	≤1 Working Day	≤3 Working Days	≤5 Working Days	Not Applicable
100	>1 Working Day & ≤2 Working Days	>3 Working Days & ≤6 Working Days	>5 Working Days & ≤10 Working Days	
200	>2 Working Days & ≤3 Working Days	>6 Working Day & ≤9 Working Days	>10 Working Day & ≤15 Working Days	
300	>3 Working Days & ≤4 Working Days	>9 Working Days & ≤12 Working Days	>15 Working Days & ≤20 Working Days	
400	>4 Working Days & ≤5 Working Days	>12 Working Days & ≤15 Working Days	>20 Working Days & ≤25 Working Days	
500	>5 Working Days & ≤6 Working Days	>15 Working Days & ≤18 Working Days	>25 Working Days & ≤30 Working Days	
100	per additional Working Day or part thereof	per additional 3 Working Days or part thereof	per additional 5 Working Days or part thereof	

3. Request Fulfilment

SLA 12 – TS Project Request	
Description	A measure of a TS Project Request that is placed with the Supplier that is accepted and completed within the target.
Calculation	Provide to the Authority a TS Project Proposal in response to a Project Request within the TS Service Level Target for Approval, subject to the volume of TS Project Requests at any given time then the Authority and Supplier shall act reasonably and negotiate in good faith as to an alternative response time. Guidance in respect of the TS Project Request classification is set out below:

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	<u>Small Change</u> • No change to an existing solution; • Small consultancy type assignment for time and materials and managed by Authority resources or no Project Management required; • There are no requirements to gain input or quotation from any other Supplier; • Something the Supplier is familiar with/has expertise in; • Accurate estimate of person days and cost can be established quickly; • No dependencies on in-flight projects. <u>Medium Change</u> • A minor modification to an existing aspect of the Transitional Services • Impact to multiple End Users • Requires Project Management resource from an Other Supplier • Participation required from two or more Other Suppliers • Minor links to in-flight projects • Requires technical subject matter expertise from at least one Other Supplier • Solution can contain the provision of hardware or software • May require a TS Contract Change • May require on-going service charge as the result of the implementation of hardware, software or service <u>Large Change</u> • May involve bespoke development requiring design and development coordination across one or more Other Suppliers • Project management resource required from one or more Other Suppliers • May involve the procurement of specialist consultant expertise to assist in the development and implementation • Considered a long-term piece of work requiring dedicated resources • May require a TS Contract Change
Exclusions	None.

ANNEX 3 (TS PERFORMANCE LEVELS) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Service Measurement Period	The Service Measurement Period (SMP) for this service is one calendar month.
TS Service Level Target	Small Change ≤ 15 Working Days Medium Change ≤ 25 Working Days Large Change ≤ 35 Working Days
TS Service Level Threshold	Not Applicable
TS Service Credit Points	Not Applicable

SLA 13 – WAN Site Provisioning		
Description	Number of Working Days from receipt of TS Project Request for a Site WAN connection (subject to the availability of existing fibre) to installation of such WAN Site connection service.	
Calculation	TS Service Credit Points shall apply for each Working Day or part thereof above the TS Service Level Target.	
TS Service Line	TS Service Level Target	TS Service Credit Points
MPLS at or below ten (10) Mbps	30 Working Days	100
MPLS greater than ten (10) Mbps	45 Working Days	100

4. TS Key Performance Indicators

The Supplier shall work with the Other Suppliers to deliver the Transitional Services to the TS KPIs as set out below.

Any TS Service Credit Points set out in the TS KPI tables below shall only apply when the TS KPI has been promoted to a TS Service Level Target.

TS KPI 1 – Severity Level 4 TS Incident Resolution	
Description	Severity Level 4 TS Incidents reported to the Supplier that are resolved within five (5) Working Days of being reported to the Supplier.
Calculation	The total number of Severity 4 TS Incidents that are resolved within five (5) Working Days of being reported to the Supplier shall be calculated and expressed as a percentage of the total number of Severity 4 TS Incidents resolved:

ANNEX 3 (TS PERFORMANCE LEVELS) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	$A / B \times 100$ Where: A = the aggregate number of Severity Level 4 TS Incidents resolved by the Supplier within the five (5) Working Day period or less within the SMP (whether such Severity Level 4 TS Incidents were reported to the Supplier in that SMP or an earlier SMP). B = the aggregate number of Severity Level 4 TS Incidents reported to and resolved within the SMP (whether such Severity Level 4 TS Incidents were reported to the Supplier in that SMP or an earlier SMP). For the avoidance of doubt, should the Supplier be investigating alongside the Authority or third party service provider, the Supplier will retain the TS Incident and include time spent in the measurement calculation. Time during which the TS Incident was not assigned to the Supplier in the TS Incident Management System should be excluded from the calculation in accordance with Paragraph 3.4(f) of this Annex 3 (<i>TS Performance Levels</i>), except where the TS Incident has been incorrectly re-assigned to another party for resolution.
Service Measurement Period	The Service Measurement Period (SMP) for this service is one calendar month. The SLA measurement time shall be as per the Service Hours defined in Table 1 of Paragraph 2.2(e).
TS KPI Target	95% within five (5) Working Days
TS Service Credit Increment	n/a
TS Service Credit Points	n/a
TS KPI 2 – Operational Changes	
Description	Number of successful changes completed in the SMP.
Calculation	$A / B \times 100$ where: A = The number of changes completed successfully B = The total number of changes requested Successful is defined as implemented or backed out successfully on initial attempt.
Service Measurement Period	The Service Measurement Period (SMP) for this service is one calendar month.

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**Confidential
Contract for the provision of WAN ServicesSecurity Classification (Official)
Contract reference: [REDACTED]

TS KPI Target	98%
TS Service Credit Increment	TS Service Credit Points shall apply for every 1% or part thereof below the TS KPI Target.
TS Service Credit Points	40 points per TS Service Credit Increment

TS KPI 3 – Problem Management	
Description	Problems raised by the Supplier or reported to the Supplier where the Root Cause Analysis (RCA) report is issued within ten (10) Working Days.
Calculation	$A / B \times 100$ where: A = The number Problems raised with RCA raised within 10 working days B = The total number of Problems raised.
Service Measurement Period	The Service Measurement Period (SMP) for this service is one calendar month.
TS KPI Target	98%
TS Service Credit Increment	1%
TS Service Credit Points	60
TS KPI 3a – Problem Management	
Description	Percentage of problem tasks completed within the agreed timescales within the SMP.
Calculation	$A / B \times 100$ where: A = The number of tasks completed in agreed timescales B = The total number of tasks agreed For the avoidance of doubt, to accommodate developing investigations, should the Supplier be investigating alongside the Authority or third party service provider, task completion dates can be changed with agreement of the MoJ Problem Manager.
Service Measurement Period	The Service Measurement Period (SMP) for this service is one calendar month.
TS KPI Target	98%
TS Service Credit Increment	1%

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

TS Service Credit Points	60

TS KPI 4 – Capacity Management – TS Incidents	
Description	Percentage of TS Incidents occurring because of insufficient service or component capacity
Service Measurement Period	The Service Measurement Period (SMP) for this service is one calendar month.
TS KPI Target	≤1%
TS Service Credit Increment	TS Service Credit Points shall apply for every 1% or part thereof above the TS Service Level Target
TS Service Credit Points	100

TS KPI 5 – Capacity Management – Utilisation	
Description	Service utilisation within +/- 5% of forecast within Capacity Plan.
Service Measurement Period	The Service Measurement Period (SMP) for this service is one calendar month.
TS KPI Target	+/-5%
TS Service Credit Increment	TS Service Credit Points shall apply for every 1% or part thereof above or below the TS Service Level Target
TS Service Credit Points	20

TS KPI 6 – Service Asset and Configuration Management - Accuracy	
Description	Accuracy of CMDB or other ITSM Toolset data.
Service Measurement Period	The Service Measurement Period (SMP) for this service is one calendar month.
TS KPI Target	≥99.9%
TS Service Credit Increment	TS Service Credit Points shall apply for every 0.1% or part thereof below the TS Service Level Target.
TS Service Credit Points	100

TS KPI 7 – Service Asset and Configuration Management - Updates	
Description	Percentage of operational updates applied to CMDB within 2 Working Days from resolution of the relevant TS Incident

ANNEX 3 (TS PERFORMANCE LEVELS) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	or completion of the relevant Service Request, Request for Service or Change
Service Measurement Period	The Service Measurement Period (SMP) for this service is one calendar month.
TS KPI Target	≥95%
TS Service Credit Increment	TS Service Credit Points shall apply for every 1% or part thereof below the TS Service Level Target.
TS Service Credit Points	100

TS KPI 8 – Request Fulfilment

Description	Requests for information, assistance or advice shall be responded to with the appropriate relevant information, assistance or advice in one (1) hour or less.
Service Measurement Period	The Service Measurement Period (SMP) for this service is one calendar month.
TS KPI Target	≥95%
TS Service Credit Increment	TS Service Credit Points shall apply for every 1% or part thereof below the TS Service Level Target.
TS Service Credit Points	40

TS KPI 9 – Patch Deployment

Description	The Supplier shall provide Vulnerability Management, as set out in Paragraph 3.5 of this Annex 3 (Performance Levels) and in accordance with the guidance only, target timescales set out below or the Vulnerability Patch Deployment Time agreed in the Vulnerability Deployment Plan.
Calculation	For each target; $A / B \times 100$ Where: A = The number of patches installed within the target timescales in the SMP in question. B = The total number of patches released within the target timescales in the SMP in question.

ANNEX 3 (TS PERFORMANCE LEVELS) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	Routine patches / updates: Standard patches and updates that are issued periodically by the manufacturer: <table> <tr> <td>Important</td><td>15 calendar days</td></tr> <tr> <td>Medium</td><td>40 calendar days</td></tr> <tr> <td>Low</td><td>90 calendar days</td></tr> </table> Critical patches: Critical patches are security software releases in response to a specific new Vulnerability should be installed within 12 calendar days. Emergency patches: Where the existence, extent, and spread of worms, viruses, or exploits poses a very high likelihood of damage to business critical systems, such as unauthorised system access, information disclosure, arbitrary code execution, or denial of service should be installed within 4 calendar days. For the avoidance of doubt, where a patch is required as a result of a Security Incident, the Security Incident response and resolution TS Service Levels shall apply.	Important	15 calendar days	Medium	40 calendar days	Low	90 calendar days
Important	15 calendar days						
Medium	40 calendar days						
Low	90 calendar days						
Service Measurement Period	The Service Measurement Period (SMP) for this service is one calendar month. The SLA measurement time shall be 15 x 7: Monday to Sunday 07:00 to 22:00.						
TS KPI Target	Routine Important Patches – 95% within fifteen (15) calendar days. Routine Medium Patches – 95% within fifteen (15) calendar days. Routine Low Patches – 95% within fifteen (15) calendar days. Critical Patches – 95% within 12 calendar days. Emergency Patches – 95% within 4 calendar days. 100% Patched as Vulnerability Patch Deployment Time agreed in the Vulnerability Deployment Plan.						
TS Service Credit Increment	n/a						
TS Service Credit Points	n/a						

**ANNEX 3 (TS PERFORMANCE LEVELS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

**ANNEX B - VULNERABILITY MANAGEMENT CLASSIFICATION AND
TIMESCALES****1. Guidance**

The Supplier shall use the Authority's ICT Security Patch Management Standard ([Patch Management Guide - Security Guidance \(justice.gov.uk\)](https://www.justice.gov.uk/patch-management-guide), and any subsequent updates) for guidance in respect of setting the Vulnerability Patch Deployment Time. An excerpt is included below.

Criticality	Description	Implementation Timescales
Routine patches / updates	Standard patches and updates that are issued periodically by the manufacturer e.g. Microsoft's "patch Tuesday" where on the second Tuesday of each month Microsoft issue patches;	Important: 15 calendar days. Medium: 30-60 calendar days. Low: 3 months.
Critical patches	Critical patches are security software releases in response to a specific new Vulnerability. Usually critical patches are released before the vulnerability is exploited and they may be released outside of the usual vendor patch cycle.	7-15 calendar days.
Emergency patches	Where the existence, extent, and spread of worms, viruses, or exploits poses a very high likelihood of damage to business critical systems, such as unauthorised system access, information disclosure, arbitrary code execution, or denial of service. Patches should be applied upon the advice of MoJ Operational Security Team and as a matter of priority.	24 hours – 4 calendar days.

End of Annex

ANNEX 4 (TS STANDARDS) to SCHEDULE 34

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

ANNEX 4

TS STANDARDS

TABLE OF CONTENTS

1. INTRODUCTION 3

2. TS BUSINESS STANDARDS 3

3. CRIMINAL JUSTICE SYSTEMS (“CJS”) DATA STANDARDS CONFORMANCE.....4

4. ENVIRONMENTAL STANDARDS 4

5. HEALTH AND SAFETY STANDARDS 4

6. INFRASTRUCTURE SAFETY STANDARDS 4

7. DATA AND INFORMATION STANDARDS 5

8. SECURITY STANDARDS 5

9. ACCESSIBLE ICT STANDARDS.....7

10. INFORMATION TECHNOLOGY STANDARDS AND REGULATIONS 7

11. ARCHITECTURE STANDARDS.....9

12. QUALITY MANAGEMENT SYSTEM STANDARDS 9

13. PORTFOLIO, PROGRAMME AND PROJECT MANAGEMENT STANDARDS.....9

14. SYSTEMS DEVELOPMENT AND INTEGRATION STANDARDS 9

15. SERVICE MANAGEMENT STANDARDS.....9

16. TESTING STANDARDS.....10

17. EXTERNAL CONNECTIVITY STANDARDS.....10

18. LANGUAGE STANDARDS.....10

19. PROCUREMENT STANDARDS.....10

20. SUPPLIER CODE OF CONDUCT 10

21. TECHNOLOGY AND DIGITAL SERVICES PRACTICE.....11

APPENDIX 1: TS SERVICE OPERATIONS MANUAL 12

ANNEX 4 (TS STANDARDS) to SCHEDULE 34

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

1. INTRODUCTION

- 1.1 In respect of the Transitional Services only, the Supplier shall comply with the TS Standards set out in this Annex 4.
- 1.2 Throughout the TS Term, the Parties shall monitor and notify each other of any new or emergent standards which could affect the Supplier's provision, or the Authority's receipt, of the Transitional Services. Any changes to the TS Standards, including the adoption of any such new or emergent standard, shall be agreed in accordance with the Change Control Procedure.
- 1.3 Where a new or emergent standard is to be developed or introduced by the Authority, the Supplier shall be responsible for ensuring that the potential impact on the Supplier's provision, or the Authority's receipt, of the Transitional Services is explained to the Authority (in a reasonable timeframe), prior to the implementation of the new or emergent standard.
- 1.4 Where TS Standards referenced conflict with each other or with Good Industry Practice, then the later TS Standard or best practice shall be adopted by the Supplier. Any such alteration to any TS Standard(s) shall require the prior written agreement of the Authority and shall be implemented within an agreed timescale.

2. TS BUSINESS STANDARDS

- 2.1 The Supplier shall comply with the business unit operating TS Standards referred to in this Paragraph 2.

HM Prison & Probation Service (HMPPS) Policies

- 2.2 Where applicable for the delivery of the Transitional Services, the Supplier shall comply with HMPPS Prison Service Orders (PSO), Prison Service Instructions (PSI) and Prison and Probation Policy Frameworks which are available at:

- Prison & Probation Policy Frameworks - GOV.UK ([www.gov.uk](https://www.gov.uk/government/collections/prison-probation-policy-frameworks))
<https://www.gov.uk/government/collections/prison-probation-policy-frameworks>
- Prison service instructions (PSIs) - GOV.UK ([www.gov.uk](https://www.gov.uk/guidance/prison-service-instructions-psis))
<https://www.gov.uk/guidance/prison-service-instructions-psis>
- Prison service orders (PSOs) - GOV.UK ([www.gov.uk](https://www.gov.uk/guidance/prison-service-orders-psos))
<https://www.gov.uk/guidance/prison-service-orders-psos>

ANNEX 4 (TS STANDARDS) to SCHEDULE 34

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

3. CRIMINAL JUSTICE SYSTEMS (“CJS”) DATA STANDARDS CONFORMANCE

Where applicable for the delivery of the Transitional Services, and especially for TS Projects in the area of data interchange with other organisations involved in the delivery of criminal justice services, the Supplier shall comply with the relevant CJS standards. The CJS standards are available at [Criminal justice system: data standards forum guidance - GOV.UK \(www.gov.uk\) \(https://www.gov.uk/guidance/criminal-justice-system-data-standards-forum-guidance\)](https://www.gov.uk/guidance/criminal-justice-system-data-standards-forum-guidance)

4. ENVIRONMENTAL STANDARDS

- 4.1 The Supplier shall comply with the environmental standards set out in Annex 1 to Schedule 4 (Standards).

5. HEALTH AND SAFETY STANDARDS

- 5.1 The Supplier shall comply with ISO 45001.

6. INFRASTRUCTURE SAFETY STANDARDS

- 6.1 The Supplier shall comply with the following standards related to the safety of information technology equipment including electrical business equipment:

6.1.1 any new hardware, required for the delivery of the Transitional Services (including printers), shall conform to BS EN IEC 62368-1:2020+A11:2020 or subsequent replacements. In considering where to site any such hardware, the Supplier shall consider the future working user environment and shall position the hardware sympathetically, wherever possible;

6.1.2 any new laser printers or scanners, required for the delivery of the Transitional Services, shall conform to BS EN 60825-1:2014 or subsequent replacement; and

6.1.3 any new apparatus for connection to any telecommunication network, and required for the delivery of the Transitional Services, shall conform to BS EN 62949:2017 or subsequent replacements.

- 6.2 Not used

- 6.3 Where required to do so, the Supplier shall be responsible for performing electrical safety checks in accordance with health and safety Law. This applies to how the checks are performed, by whom, and how frequently they should occur.

ANNEX 4 (TS STANDARDS) to SCHEDULE 34

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

6.4 The Supplier shall ensure that all equipment supplied in connection with the Transitional Services shall comply with the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 and any later amendments.

6.5 The Supplier shall comply with MoJ ICT Physical Infrastructure Standards v 4.3, as amended from time to time.

7. DATA AND INFORMATION STANDARDS

7.1 The Supplier shall comply with the ISO 8000 Data Quality standard or, where agreed with the Authority, a similar or equivalent standard.

7.2 The Supplier should comply with and use the Infrastructure Technology Library (ITIL) version 3 or above for management and governance of all information and data handling processes.

7.3 The Supplier shall comply with the ISO 22745 Exchange of Data Quality standard or, where agreed with the Authority, a similar or equivalent standard.

8. SECURITY STANDARDS

The Supplier shall ensure the Transitional Services are operated and delivered in compliance of the standards set out in this Paragraph 8.

8.1 The Supplier shall comply with HM Government and industry information assurance best practice, guidelines and requirements.

8.2 The Supplier shall ensure that all Sites containing protectively marked assets, for which the Supplier (and/or any of its Key Sub-contractors) is responsible, comply with List X standards as specified by the security policy framework (<https://www.gov.uk/government/publications/security-requirements-for-list-x-contractors>).

8.3 The Supplier shall be compliant with ISO/IEC 27001 and shall use the guidance from the following in implementing and delivering the Transitional Services:

- (a) ISO/IEC 27002 — Code of practice for information security management
- (b) ISO/IEC 27011 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- (c) ISO/IEC 27033 — Parts 1 to 4 Network security;
- (d) HMG Functional Standard GovS 007: Security Government Functional Standard GovS 007: Security - GOV.UK (www.gov.uk);

ANNEX 4 (TS STANDARDS) to SCHEDULE 34

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (e) NCSC Guidance <https://www.ncsc.gov.uk/section/advice-guidance/all-topics>;
 - (f) HMG GovAssure and Cyber Assessment Framework GovAssure - UK Government Security NCSC CAF guidance - NCSC.GOV.UK; and
 - (g) MoJ Cyber and Technical Guidance Security Guidance (justice.gov.uk).
- 8.4 The Supplier shall ensure that malware protection is in place for all Supplier TS Equipment in line with PSN Standard: Technical Standard Common Standard for Malware Protection.
- 8.5 The Supplier shall ensure that all Supplier TS Equipment is patched and maintained in line with PSN Standard: Technical Standard Common Standard for Patch Management.
- 8.6 The Supplier shall ensure the Transitional Services are delivered in compliance with:
- (a) PSN standard: Technical Standard Common Standard for Malware Protection;
 - (b) PSN standard: Technical Standard Common Standard for Patch Management;
 - (c) the PSN Operating Model v2.0, Dec 2010;
 - (d) Government Conveyance Network Service Description v4.0, Jan 2013;
 - (e) Technical Domain Description v4.0, May 2013;
 - (f) the PSN's Public Key Infrastructure Strategy – version 1.0, Jul 2011;
 - (g) the PSN's Identity Assurance Strategy – version 2.0, May 2011;
 - (h) the Supplier TS Solution shall comply with PSN Compliance v3.7, Jul 2012 and PSN Technical Domain Description V4.0;
 - (i) [REDACTED]
- [REDACTED]
- [REDACTED]
- together, the “PSN Standard”.

ANNEX 4 (TS STANDARDS) to SCHEDULE 34

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

9. ACCESSIBLE ICT STANDARDS

- 9.1 The Supplier shall comply with the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.1 Conformance Level AA.
- 9.2 The Supplier shall comply with ISO/IEC 13066-1: 2011 Information Technology – Interoperability with assistive technology (AT) – Part 1: Requirements and recommendations for interoperability.
- 9.3 The Supplier shall comply with ISO/IEC 30071-1:2019.

10. INFORMATION TECHNOLOGY STANDARDS AND REGULATIONS

- 10.1 The Supplier shall comply with standards relating to Greening government: ICT and digital services strategy 2020-2025.
- 10.2 The Supplier shall comply to the extent within its control with the UK Government's Open Standards Principles as documented at <https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles>
- 10.3 The Supplier shall ensure that all documentation published to the Authority is provided in a non-proprietary format (such as PDF or Open Document Format (ISO 26300 or equivalent) as well as any native file format in accordance with the obligation under Paragraph 10.2 to comply with the UK Government's Open Standards Principles, unless the Authority otherwise agrees in writing.
- 10.4 The Supplier shall comply where relevant with HM Government Open Standards Principles, especially as these relate to specification of standards for software interoperability, data and document formats in Government IT.
- 10.5 The Supplier shall comply with the Standards specified in the PSN including but not limited to:
- 10.5.1 the PSN Operating Model v2.0, Dec 2010;
 - 10.5.2 Government Conveyance Network Service Description v4.0, Jan 2013;
 - 10.5.3 Technical Domain Description v4.0, May 2013;
 - 10.5.4 the PSN's Public Key Infrastructure Strategy – version 1.0, Jul 2011; and
 - 10.5.5 the PSN's Identity Assurance Strategy – version 2.0, May 2011.

ANNEX 4 (TS STANDARDS) to SCHEDULE 34

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 10.6 The Supplier shall comply with the international industry standards for data centres, including:
- 10.6.1 BS EN 50600 (2021): Information technology. Data centre facilities and infrastructures;
 - 10.6.2 ANSI/TIA-942-A-1 (2013): Telecommunications Infrastructure Standards for Data Centers;
 - 10.6.3 IEC 60297-3-100: Mechanical structures for electronic equipment – Dimensions of mechanical structures of the 482,6 mm (19 in) series;
 - 10.6.4 ASHRAE, Best Practice for Datacom Facility Energy Efficiency, Second Edition (2009);
 - 10.6.5 ASHRAE, Design Considerations for Data and Communications Equipment Centers, Second Edition (2009); and
 - 10.6.6 ASHRAE 2011, Thermal Guidelines for Data Processing Environments – Expanded Data Centre Classes and Usage Guidance, 2011.
- 10.7 The Supplier shall comply with the EU Code of Conduct on Data Centres Energy Efficiency. The Supplier shall ensure that any data centres used in delivering the Transitional Services are registered as a participant under the Code of Conduct.
- 10.8 The Supplier shall comply with the Authority and HM Government's objectives to reduce waste and meet the aims of the Greening Government: ICT Strategy contained in the document "Greening government: ICT and digital services strategy 2020-2025 The latest official version can be found at: [Greening government: ICT and digital services strategy 2020-2025 - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/publications/greening-government-ict-and-digital-services-strategy-2020-2025/greening-government-ict-and-digital-services-strategy-2020-2025) (<https://www.gov.uk/government/publications/greening-government-ict-and-digital-services-strategy-2020-2025/greening-government-ict-and-digital-services-strategy-2020-2025>)
- 10.9 The Supplier shall comply with the Authority's Digital Strategy and UK Government Sustainable Development Goals, as updated from time to time.
- 10.10 The Supplier shall ensure that the Transitional Services will take account of best practice from The National Archive for Email Archiving. The latest version can be found at: <https://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/managing-email/>.
- 10.11 The Supplier shall comply with IEEE 802.1X for all Network Access Control capabilities.

ANNEX 4 (TS STANDARDS) to SCHEDULE 34

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

11. ARCHITECTURE STANDARDS

- 11.1 The Supplier shall produce full and detailed technical architecture documentation for the Supplier TS Solution in accordance with Good Industry Practice. If documentation exists that complies with the Open Group Architecture Framework 9.2 or its equivalent and the Open-Enterprise Security Architecture (O-ESA) Architecture Framework and Standards, then this shall be deemed acceptable.

12. QUALITY MANAGEMENT SYSTEM STANDARDS

- 12.1 The Supplier shall comply with either HM Government Standards for Quality Management, e.g. ISO 9001 or other best industry Standards as agreed and documented in the Quality Management System.

13. PORTFOLIO, PROGRAMME AND PROJECT MANAGEMENT STANDARDS

- 13.1 The Supplier shall comply with the Authority's Project Delivery Standard, supplemented where appropriate by the tools and methods of the Supplier's own project management methodologies.
- 13.2 The Supplier shall make use of the COBIT framework for business / IT alignment and the CMMI framework for organisational maturity assessment.

14. SYSTEMS DEVELOPMENT AND INTEGRATION STANDARDS

- 14.1 Where applicable for the delivery of the Transitional Services, and especially in the area of data interchange with other organisations involved in the delivery of criminal justice services, the Supplier shall comply with CCCJS/IBIS Standards and principles. The Authority shall make these available to the Supplier.
- 14.2 The Supplier shall comply with the Digital By Default Service Standard as set out at: <https://www.gov.uk/service-manual/digital-by-default>.

15. SERVICE MANAGEMENT STANDARDS

- 15.1 The Supplier shall comply with Industry and HM Government Standards and best practice guidelines in the delivery of the Transitional Services including but not limited to:
- 15.1.1 ITIL v3 2011 or later;
 - 15.1.2 ISO/IEC 20000-1 2018 "Information technology – Service management – Part 1";
 - 15.1.3 ISO/IEC 20000-2 2019 "Information technology — Service management – Part 2";

ANNEX 4 (TS STANDARDS) to SCHEDULE 34

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

15.1.4 ISO 10007 “Quality management systems – Guidelines for configuration management”; and

15.1.5 ISO 22313:2020 “Security and resilience. Business continuity management systems. Guidance on the use of ISO 22301” and, ISO/IEC 27031:2011, ISO 22301 and ISO/IEC 24762:2008 in the provision of ITSC/DR plans.

16. TESTING STANDARDS

16.1 The Supplier shall comply with the relevant TS Project Test Strategy when delivering a TS Project.

16.2 The Supplier shall comply with the Agreed Test Strategy for Exit and Migration of the Transitional Services as set out in the existing Detailed Implementation Plan.

17. EXTERNAL CONNECTIVITY STANDARDS

17.1 The Supplier TS Solution shall comply with PSN Compliance v3.7, Jul 2012 and PSN Technical Domain Description V4.0.

18. LANGUAGE STANDARDS

18.1 The Supplier shall ensure that all Transitional Services comply with the Welsh Language Act 1993 and the Welsh Language (Wales) Measure 2011.

19. PROCUREMENT STANDARDS

19.1 The Supplier shall meet the applicable Government Buying Standards applicable to the Transitional Services which can be found online at:

<https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs>

20. SUPPLIER CODE OF CONDUCT

20.1 In February 2019, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government which can be found online at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1163536/Supplier_Code_of_Conduct_v3.pdf.The

Authority expects to meet, and expects the Supplier to meet, the standards set out in that Code.

ANNEX 4 (TS STANDARDS) to SCHEDULE 34

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

21. TECHNOLOGY AND DIGITAL SERVICES PRACTICE

- 21.1 The Supplier shall (when designing, implementing, and delivering the Transitional Services) adopt the applicable elements of HM Government's Technology Code of Practice as documented at <https://www.gov.uk/service-manual/technology/code-of-practice.html>

ANNEX 4 (TS STANDARDS) to SCHEDULE 34
Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

	[REDACTED]
	[REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]		
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

[illegible]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED] [REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible][illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

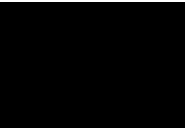
Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]



**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**



Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]		
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]		
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]



**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

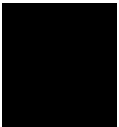
[REDACTED]

[REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



[REDACTED]

[REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential

	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]



**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official) [REDACTED]
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official
Contract reference: [REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

[REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

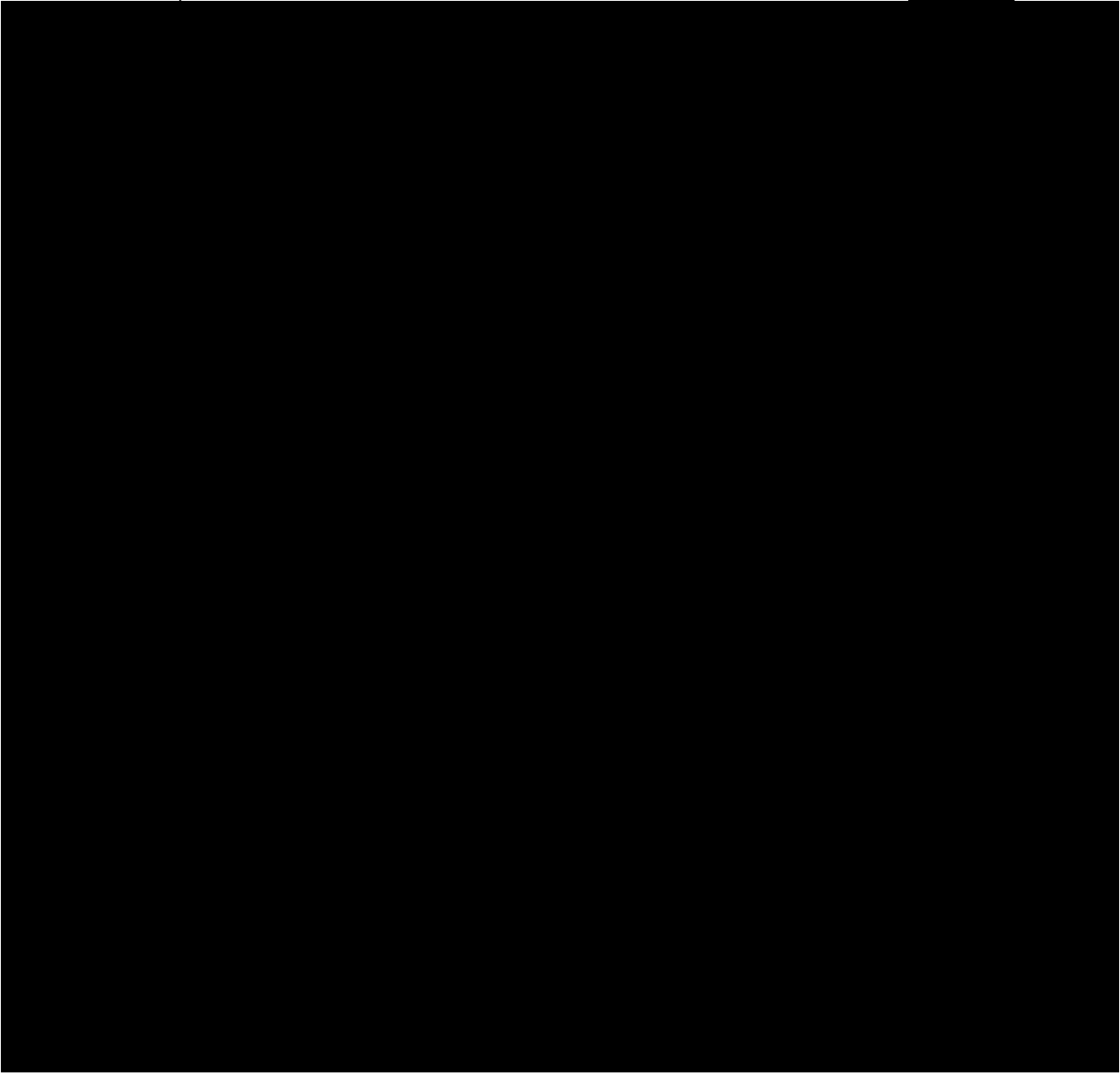
Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

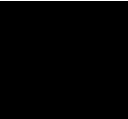
**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**



Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]



**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference:

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

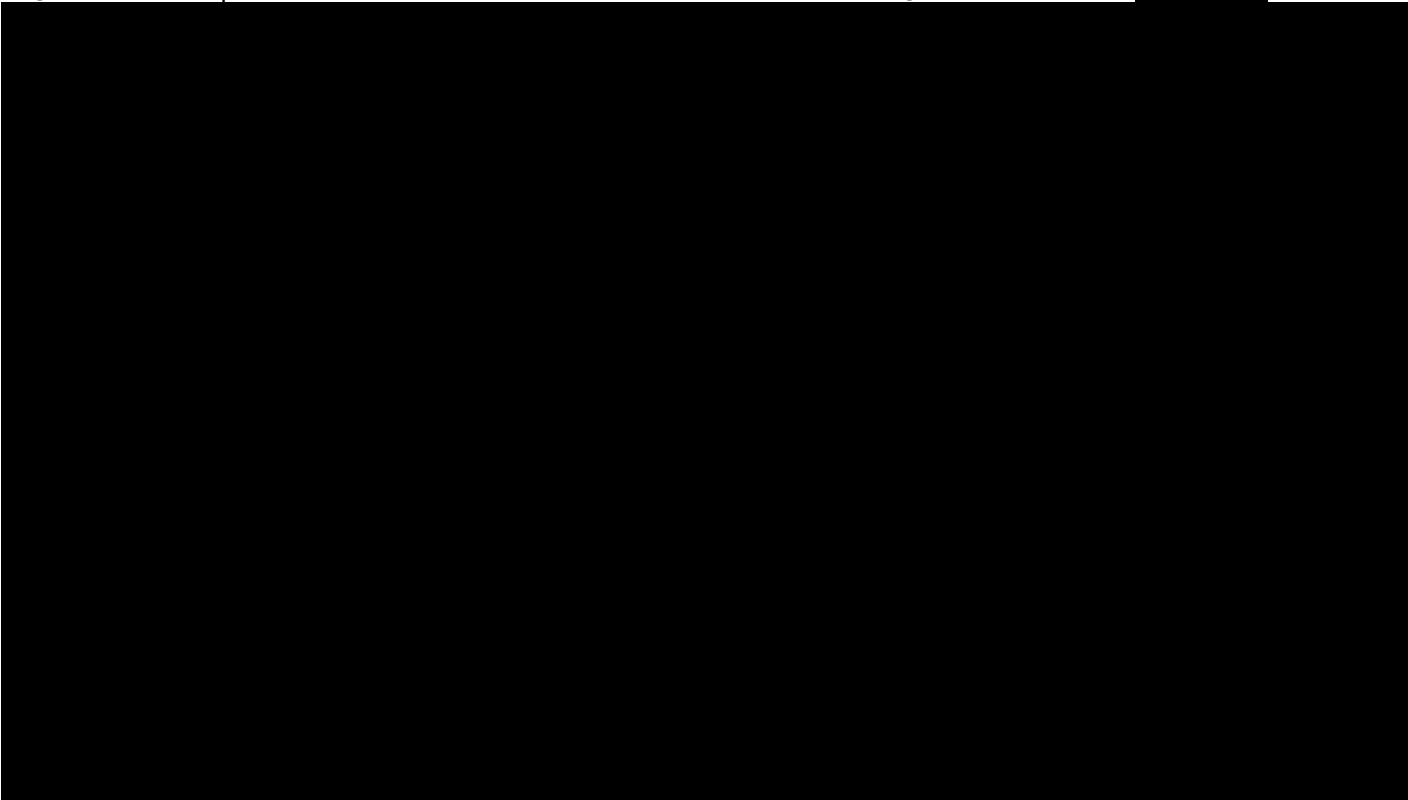
[illegible]

35

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official
Contract reference: [Redacted]



[Redacted]

[Redacted]

[Redacted]		[Redacted]
[Redacted]	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	
	[Redacted]	
	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

Security Classification (Official)
Contract reference: [REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official [REDACTED])
Contract reference: [REDACTED]

		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential

Contract for the provision of WAN Services

Security Classification (Official

Contract reference:

[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official
Contract reference: [REDACTED])

A 10x10 grid of 100 squares. Each square contains a small black square in the top-left corner, representing a sparse matrix. The black squares are arranged in a pattern that suggests a lower triangular matrix with some off-diagonal elements.

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

A 10x10 grid of 100 squares. Each square contains a smaller black or white square, creating a complex, abstract pattern. The pattern is composed of various shapes, including lines, dots, and larger blocks, arranged in a way that suggests a larger, more complex structure. The overall effect is a dense, textured composition of black and white elements.

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	
		[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference:

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]

[REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible][illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

								T			
[REDACTED]	[REDACTED]						[REDACTED]	[REDACTED]			
[REDACTED]	[REDACTED]						[REDACTED]	[REDACTED]			

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Office [Redacted])
Contract reference: [Redacted]

[Redacted]

[Redacted]		
[Redacted]		
[Redacted]	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]
	[Redacted]	[Redacted]

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official
Contract reference: [REDACTED])

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

		1 [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official) [REDACTED]
Contract reference: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]
		[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED] [REDACTED]

1

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

		1. [REDACTED] 2. [REDACTED] 3. [REDACTED] 4. [REDACTED] 5. [REDACTED] 6. [REDACTED] 7. [REDACTED] 8. [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED] [REDACTED] 1. [REDACTED] 2. [REDACTED] 3. [REDACTED] 4. [REDACTED] 5. [REDACTED] 6. [REDACTED] 7. [REDACTED] 8. [REDACTED] 9. [REDACTED] 10. [REDACTED] 11. [REDACTED] 12. [REDACTED] 13. [REDACTED] 14. [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] 1. [REDACTED] 2. [REDACTED] 3. [REDACTED] 4. [REDACTED] 5. [REDACTED] 6. [REDACTED] 7. [REDACTED] 8. [REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[REDACTED]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [Redacted]

[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

[Redacted]

[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible][illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

[illegible]

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

1		
2		
3		
4		
5		
6		
7		
8		

**APPENDIX 1 (TS SERVICE OPERATIONS MANUAL) to
ANNEX 4 (TS STANDARDS) to SCHEDULE 34**

Confidential
Contract for the provision of WAN Services

Security Classification (Official
Contract reference: [REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]



ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

ANNEX 5

TS SECURITY MANAGEMENT

Part A: TS Security Assurance 3

1. Definitions and Order of Precedence 3

2. Introduction 7

3. Principles of Security 8

4. TS Information Management System 10

5. TS Statement of Information Risk Appetite and TS Baseline Security Requirements 11

6. TS Security Assurance of the TS Core Information Management System.....11

7. TS Certification Requirements.....16

8. TS Security Testing 18

9. Not used 22

10. Malicious Software 22

11. TS Breach of Security.....23

12. Data Processing, Storage, Management and Destruction 24

13. Security Monitoring and Reporting 25

APPENDIX 1: TS BASELINE SECURITY REQUIREMENTS.....26

APPENDIX 2: TS SUB-CONTRACTOR SECURITY REQUIREMENTS 44

APPENDIX 3: TS SECURITY MANAGEMENT PLAN TEMPLATE 49

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Part A: TS Security Assurance**1. Definitions and Order of Precedence****1.1 In this Annex:**

“Anti-Malicious Software”	means software that scans for and identifies possible Malicious Software in the TS IT Environment;
“Authority TS Security Representative”	means the single point of contact, nominated by the Authority, who has overall responsibility for security in relation to the Transitional Services;
“CHECK Service Provider”	means a company which has been certified by the National Cyber Security Centre, holds “Green Light” status and is authorised to provide the IT Health Check services required by Paragraph 8.1;
“Commercial off the shelf Software” or “COTS Software”	means commercial off the shelf software in use for the provision and support of the Transitional Services, and includes the TS COTS Software and the TS Third Party COTS Software;
“CREST Service Provider”	means a company with a SOC Accreditation from CREST International;
“Cyber Essentials”	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;
“Cyber Essentials Plus”	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
“Cyber Essentials Scheme”	means the Cyber Essentials scheme operated by the National Cyber Security Centre;
“Existing Security Measures”	shall have the meaning given in Paragraph 3.9 of this Schedule 5;
“Existing Services”	shall have the meaning given in Paragraph 3.9 of this Schedule 5;
“IT Health Check”	has the meaning given Paragraph 8.1.1;
“Process”	means any operation which is performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

“Remediation Action Plan”

has the meaning given in Paragraph 8.3.3(a);

“Special Category Personal Data”

means the categories of Personal Data set out in article 9(1) and article 10 of the UK GDPR;

“Statement of Information Risk Appetite”

has the meaning given in Paragraph 5.1;

“Supplier TS Security Representative”

means the single point of contact, who shall be a member of the TS Key Personnel, nominated by the Supplier and approved by the Authority, who has overall responsibility for security assurance in relation to the Transitional Services;

“TS Baseline Security Requirements”

the baseline security requirements, the current copy of which is contained in Appendix 1 (*TS Baseline Security Requirements*), updated from time to time and notified to the Supplier in accordance with Paragraph 18 of this Schedule 34;

“TS Breach of Security”

means the occurrence of:

- (a) any unauthorised access to or use of the Transitional Services, the Supplier Premises, the Authority Premises, the Sites, the Supplier TS System, the Authority System and/or any information or data (including the Confidential Information and the Authority Data and/or the) used by the Authority, the Supplier, or any Sub-contractor in connection with this Schedule 34;
- (b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including copies of such information or data, used by the Authority, the Supplier, or any Sub-contractor in connection with this Schedule 34; and/or
- (c) any part of the Supplier TS System ceasing to be compliant with the TS Certification Requirements,

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

in each case as more particularly set out in the security requirements in the TS Baseline Security Requirements;

“TS Certification Requirements”

means the information security requirements set out in Paragraph 7;

“TS CIMS Sub-contractor”

means a Sub-contractor that provides or operates the whole, or a substantial part, of the TS Core Information Management System;

“TS Core Information Management System”

means those information assets, IT systems and/or Sites which will be used by the Supplier and/or its Sub-contractors to Process Authority Data, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources) which the Authority has determined in accordance with Paragraph 4.2 shall be subject to the TS Baseline Security Requirements;

“TS Higher Risk Sub-contractor”

means a Sub-contractor that Processes Authority Data where that data includes either:

- (a) the Personal Data of 1000 or more individuals in aggregate during the period between the Transitional Services Commencement Date and the end of the TS Term; or
- (b) any part of that data includes any of the following:
 - (i) financial information (including any tax and/or welfare information) relating to any person;
 - (ii) any information relating to actual or alleged criminal offences (including criminal records);
 - (iii) any information relating to children and/or vulnerable persons;
 - (iv) any information relating to social care;
 - (v) any information relating to a person's current or past employment; or
 - (vi) Special Category Personal Data; or

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- (c) the Authority in its discretion, designates a Sub-contractor as a TS Higher Risk Sub-Contractor; or
- (d) the Authority considers, in its discretion, that any actual or potential Processing carried out by the Sub-contractor is high risk;

“TS Information Management System”

means the TS Core Information Management System and the TS Wider Information Management System;

“TS Medium Risk Sub-contractor”

means a Sub-contractor that Processes Authority Data, where that data

- (a) includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the Transitional Services Commencement Date and the end of the TS Term; and
- (b) does not include Special Category Personal Data;

“TS Required Changes Register”

means the register forming part of the TS Security Management Plan which records each of the changes that the Supplier has agreed with the Authority shall be made to the TS Core Information Management System and/or the TS Security Management Plan as a consequence of the occurrence of any of the events set out in Paragraph 6.14 together with the date on which each such change shall be implemented and the date on which each such change was implemented;

“TS Residual Risk Statement”

means a notice issued by the Authority which sets out the information risks associated with using the TS Core Information Management System and confirms that the Authority is satisfied that the identified risks have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Authority;

“TS Risk Management Rejection Notice”

has the meaning given in Paragraph 6.8.2;

“TS Security Assurance”

means the assessment of the Transitional Services and the TS Core Information Management System in accordance with Paragraph 6 by the Authority or by

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

representatives appointed by the Authority, which results in a TS Security Assurance Decision;

“TS Security Assurance Decision”	means the decision of the Authority, taken in accordance with the process set out in Paragraph 6, to issue the Supplier with a TS Residual Risk Statement or a TS Risk Management Rejection Notice in respect of the Transitional Services and the TS Core Information Management System;
“TS Security Assurance Plan”	means the Supplier’s plan to attain a TS Residual Risk Statement from the Authority, which is prepared by the Supplier and approved by the Authority in accordance with Paragraph 6.6;
“TS Security Management Plan”	has the meaning given in Paragraph 6.5;
“TS Security Test”	has the meaning given Paragraph 8.1;
“TS Sub-contractor Security Requirements”	means those requirements set out in Appendix 2; and
“TS Wider Information Management System”	means those information assets, IT systems and/or Sites which will be used by the Supplier and/or its Sub-contractors to Process Authority Data which have not been determined by the Authority to form part of the TS Core Information Management System, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources).

- 1.2 If there is any conflict between this Annex 5 (*TS Security Management*) and the TS Baseline Security Requirements, then this Annex 5 shall prevail unless expressly stated otherwise in the TS Baseline Security Requirements.

2. Introduction

- 2.1A The Authority operates an integrated, through-life process in partnership with suppliers which is transparent, auditable, and consistently applied to safeguard the Authority’s data and services. This process is simply termed ‘Security Assurance’ and it is scoped to provide Security Assurance across suppliers, supply chain, and both the TS Wider Information Management System and the TS Core Information Management System.
- 2.1B Security Assurance is underpinned by GovAssure and is aligned to the Authority’s risk appetite. GovAssure provides Government organisations and their security functions with an effective mechanism to understand the level of

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

cyber resilience and provide a common baseline level of resilience to achieve for new and existing services in line with:

- 2.1B.1 the HMG and Authority Cyber Security Strategy which can be found at: <https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030>; and
 - 2.1B.2 the Authority's strategy which can be found at: <https://www.gov.uk/government/publications/ministry-of-justice-cyber-security-strategy-2023-to-2028>.
- 2.1C Through GovAssure, organisations are required to actively manage and report on the cyber capability, risk and resilience of their supply chain, networks, and systems. GovAssure specifies appropriate security outcomes defined by threat driven [Government-specific profiles under the Cyber Assessment Framework \(CAF\) \(Baseline and Enhanced\)](#). GovAssure is accompanied by centralised cyber security policy and guidance for Government to support best practice.
- 2.1 This Part A of this Schedule sets out:
- 2.1.1 the arrangements the Supplier must implement before, and comply with when, providing the Transitional Services and performing its other obligations under this Schedule 34 to ensure the security of the Authority Data, the TS IT Environment, the Transitional Services and the TS Information Management System;
 - 2.1.2 the process which shall apply to the TS Security Assurance of the TS Core Information Management System in Paragraph 6;
 - 2.1.3 the TS Certification Requirements applicable to the TS Wider Information Management System in Paragraph 7;
 - 2.1.4 the TS Security Tests which the Supplier shall conduct during the TS Term in Paragraph 8;
 - 2.1.5 the TS Security Tests which the Authority may conduct during the TS Term in Paragraph 8.6;
 - 2.1.6 not used;
 - 2.1.7 the obligations on the Supplier to prevent the introduction of Malicious Software into the TS Information Management System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the TS Information Management System in Paragraph 10; and
 - 2.1.8 each Party's obligations in the event of an actual or attempted TS Breach of Security in Paragraph 11.

3. Principles of Security

- 3.1 The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Authority Data and, consequently

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

on the security of:

- 3.1.1 the Sites;
 - 3.1.2 the TS IT Environment;
 - 3.1.3 the TS Core Information Management System; and
 - 3.1.4 the Transitional Services.
- 3.2 Notwithstanding the involvement of the Authority in the TS Security Assurance of the Transitional Services, the Supplier, Sub-contractors and the TS Core Information Management System, the Supplier shall be and shall remain responsible for:
- 3.2.1 the security, confidentiality, integrity and availability of the Authority Data whilst that Authority Data is under the control of the Supplier or any of its Sub-contractors; and
 - 3.2.2 the security of the TS Information Management System.
- 3.3 The Supplier shall:
- 3.3.1 comply with the TS Baseline Security Requirements; and
 - 3.3.2 not used;
 - 3.3.3 ensure that all Sub-contractors that Process Authority Data comply with the TS Sub-contractor Security Requirements.
- 3.3A The Supplier shall ensure that the Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Annex 5, including any requirements imposed on Sub-contractors by Appendix APPENDIX 2, from the Transitional Services Commencement Date.
- 3.4 "Security management" shall be included on the agenda of the relevant Board(s) (as determined by the Authority) in order to discuss and monitor security matters including:
- 3.4.1 the TS Security Assurance of the TS Core Information Management System; and
 - 3.4.2 recommendations related to the TS Security Assurance of the TS Core Information Management System.
- 3.5 To facilitate the Supplier's design, implementation, operation, management and continual improvement of the TS Security Management Plan and the security of the Transitional Services, the TS Information Management System and otherwise:
- 3.5.1 the Supplier shall provide access to the Supplier Personnel responsible for information assurance; and
 - 3.5.2 the Authority shall provide access to its personnel responsible for

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

information assurance,

in each case at reasonable times on reasonable notice.

3.6 The Authority shall appoint an Authority TS Security Representative and the Supplier shall appoint a Supplier TS Security Representative. The Authority TS Security Representative and the Supplier TS Security Representative shall be appropriately qualified, competent and empowered to take action to safeguard the Authority Data.

3.7 The Supplier TS Security Representative shall:

3.7.1 be a suitably qualified individual acting as the SPOC for all security matters in relation to the Transitional Services, and whose purpose and role is to co-ordinate with the appropriate resources and functions within the Supplier that develops, implements and maintains the cybersecurity and privacy controls;

3.7.2 ensure cybersecurity and privacy controls relevant to the TS Information Management System are in place, effective, and documented with appropriate context in the TS Security Management Plan; and,

3.7.3 ensure that mechanisms are in place at all times to review cybersecurity and privacy controls, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

3.8 The Authority TS Security Representative shall be the primary point of contact for the Supplier TS Security Representative.

3.9 The Parties acknowledge that, in relation to the Preceding Services which the Authority was receiving from the Supplier immediately prior to the Effective Date ("**Existing Services**"), the Supplier agreed certain security management measures and obligations (including a security management plan and risk register) with the Authority as part of the contract governing the provision of those Existing Services (the "**Existing Security Measures**"). Pending approval of the TS Security Management Plan by the Authority in accordance with Paragraph 6, the Supplier will continue to comply with the Existing Security Measures unless expressly agreed otherwise in writing with the Authority.

4. TS Information Management System

4.1 The TS Information Management System comprises the TS Core Information Management System and the TS Wider Information Management System.

4.2 The Authority shall be responsible for determining the boundary between the TS Core Information Management System and the TS Wider Information Management System. The Supplier shall be responsible for documenting the boundary between the TS Core Information Management System and the TS Wider Information Management System. In order to enable the Authority to

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

make such determination, the Supplier shall provide the Authority with an appropriately detailed diagram of the TS Information Management System together with such documentation and information that the Authority may reasonably require regarding any information assets, IT systems and/or Sites which will be used by the Supplier or any Sub-contractor to Process Authority Data together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources).

- 4.3 The Authority shall notify the Supplier, as soon as reasonably practical following the receipt of such documentation and information, of the Authority's decision regarding the component parts of the TS Core Information Management System and its boundary with the TS Wider Information Management System.
- 4.4 The Supplier shall reproduce the Authority's decision as a diagram documenting the TS Core Information Management System, the TS Wider Information Management system and the boundary between the two. This diagram shall form part of the TS Security Management Plan.
- 4.5 Any proposed change to the component parts of the TS Core Information Management System or the boundary between the TS Core Information Management System and the TS Wider Information Management System shall be notified and processed in accordance with the Change Control Procedure.
- 4.6 Not used.
- 4.7 Not used.
- 4.8 The Supplier shall comply with any limitations specified by the Authority on use of the TS Information Management System to Process Authority Data.

5. TS Statement of Information Risk Appetite and TS Baseline Security Requirements

- 5.1 The Supplier acknowledges that the Authority will provide and the Supplier will acknowledge receipt of the Authority statement of information risk appetite for the Supplier TS System and the Transitional Services (the "**TS Statement of Information Risk Appetite**").
- 5.2 The TS Baseline Security Requirements in respect of the TS Core Information Management System are set out in Appendix 1.

6. TS Security Assurance of the TS Core Information Management System

- 6.1 The TS Core Information Management System shall be subject to TS Security Assurance in accordance with this Paragraph 6.
- 6.2 The Supplier acknowledges that the purpose of TS Security Assurance of the TS Core Information Management System is to ensure that:
 - 6.2.1 the TS Security Management Plan accurately represents the TS Core

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Information Management System;

- 6.2.2 the TS Security Assurance Plan, if followed, provides the Authority with sufficient confidence that the TS Core Information Management System will meet the TS Baseline Security Requirements and the TS Statement of Risk Appetite;
- 6.2.3 the security related mobilisation activities to be delivered by the Supplier are as set out in the Implementation Plan; and
- 6.2.4 the residual risks of the TS Core Information Management System are no greater than those provided for in the TS Statement of Risk Appetite and the TS Baseline Security Requirements.
- 6.3 The TS Security Assurance shall be performed by the Authority or by representatives appointed by the Authority. The Supplier shall provide such information as is reasonably required by the Authority in relation to such TS Security Assurance process.
- 6.4 In addition to any obligations imposed by Schedule 13 (*Implementation*) or Schedule 14 (*Testing Procedures*) the Supplier must ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Annex, including any requirements imposed on Sub-contractors by Appendix APPENDIX 2, from the Transitional Services Commencement Date.
- 6.5 By the date specified in the Implementation Plan for the submission of the Security Management Plan, the Supplier shall prepare and submit to the Authority the risk management documentation for the TS Core Information Management System, which shall be subject to approval by the Authority in accordance with this Paragraph 6 (the "**TS Security Management Plan**").
- 6.6 The TS Security Management Plan shall be structured in accordance with the template as set out in Appendix APPENDIX 3 to this Annex and include:
 - 6.6.1 the TS Security Assurance Plan, which shall include:
 - (a) the dates on which each subsequent iteration of the TS Security Management Plan will be delivered to the Authority for review and staged approval in line with the Implementation Plan; and
 - (b) the date by which the Supplier is required to have received a TS Residual Risk Statement together with details of each of the tasks which must be completed by the Supplier and the Authority Responsibilities which must be completed in order for the Supplier to receive a TS Residual Risk Statement pursuant to Paragraph 6.11;
 - 6.6.2 a formal risk assessment of the TS Core Information Management System and a risk treatment plan for the TS Core Information Management System, in each case containing the details set out in Appendix 3 (*TS Security Management Plan Template*) to this Annex 5;

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- 6.6.3 a completed ISO/IEC 27001 (at least ISO/IEC 27001:2013) Statement of Applicability for the TS Core Information Management System;
- 6.6.4 the process for managing any security risks from Sub-contractors and third parties authorised by the Authority with access to the Transitional Services, processes associated with the delivery of the Transitional Services, the Authority Premises, the Sites, the Supplier TS System, the Authority System (to extent that it is under the control of the Supplier) and any IT, Information and data (including the Confidential Information of the Authority and the Authority Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Transitional Services;
- 6.6.5 unless such requirement is waived by the Authority, proposed controls that will be implemented in respect of all aspects of the Transitional Services and all processes associated with the delivery of the Transitional Services, including the Authority Premises, the Sites, the Supplier TS System, the Authority System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Confidential Information of the Authority and the Authority Data) to the extent used by the Authority or the Supplier in connection with this Schedule 34 or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Transitional Services;
- 6.6.6 the TS Required Changes Register;
- 6.6.7 evidence that the Supplier and each applicable Sub-contractor is compliant with the TS Certification Requirements; and
- 6.6.8 the diagram documenting the TS Core Information Management System, the TS Wider Information Management System and the boundary between them created under Paragraph 4.1.
- 6.7 To facilitate TS Security Assurance of the TS Information Management System, the Supplier shall provide the Authority and its authorised representatives with:
 - 6.7.1 access to the Sites, ICT information assets and ICT systems within the TS Core Information Management System on request or in accordance with the TS Security Assurance Plan ; and
 - 6.7.2 such other information and/or documentation that the Authority and/or its authorised representatives may reasonably require, to enable the Authority to establish that the TS Core Information Management System is compliant with the TS Security Management Plan.
- 6.8 The Authority shall, by the relevant date set out in the TS Security Assurance Plan, review the TS Security Management Plan and issue to the Supplier either:
 - 6.8.1 a TS Residual Risk Statement which will then form part of the TS

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Security Management Plan, confirming that the Authority is satisfied that the identified risks to the TS Core Information Management System have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Authority; or

- 6.8.2 a rejection notice stating that the Authority considers that the identified risks to the TS Core Information Management System have not been adequately or appropriately addressed, or the residual risks to the TS Core Information Management System have not been reduced to the level anticipated by the TS Statement of Information Risk Appetite, and the reasons why ("**TS Risk Management Rejection Notice**").
- 6.9 If the Authority issues a TS Risk Management Rejection Notice, the Supplier shall, within 20 Working Days of the date of the TS Risk Management Rejection Notice:
- 6.9.1 comply with any limitations specified by the Authority on use of the TS Information Management System to Process Authority Data
- 6.9.2 address all of the issues raised by the Authority in such notice;
- 6.9.3 update the TS Security Management Plan, as appropriate; and
- 6.9.4 notify the Authority that the TS Core Information Management System is ready for a TS Security Assurance Decision.
- 6.10 If the Supplier is issued with two or more TS Risk Management Rejection Notices, the Authority shall be entitled to require the Supplier to prepare (at the Supplier's expense) an update to the TS Security Management Plan for review by the Authority in accordance with this Paragraph 6 (including providing the Authority and its authorised representatives with access, information and documentation as set out in Paragraph 6.7).
- 6.11 Subject to Paragraph 6.10, the process set out in Paragraphs 6.8 to 6.10 shall be repeated until such time as the Authority issues a TS Residual Risk Statement to the Supplier or the Authority terminates this Contract or the Transitional Services.
- 6.12 Unless agreed otherwise by the Authority, the Supplier shall not use the TS Core Information Management System to Process Authority Data before receiving a TS Residual Risk Statement.
- 6.13 The Supplier shall keep the TS Core Information Management System and TS Security Management Plan under review and shall update the TS Security Management Plan annually in accordance with this Paragraph and the Authority shall review the TS Security Assurance Decision annually and following the occurrence of any of the events set out in Paragraph 6.15.
- 6.14 The Supplier shall notify the Authority within 3 Working Days after becoming aware of:
- 6.14.1 a significant change, or a significant planned change, to the

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

components or architecture of the TS Core Information Management System;

- 6.14.2 a new risk is identified to the components or architecture of the TS Core Information Management System;
- 6.14.3 a change in the threat profile;
- 6.14.4 not used;
- 6.14.5 a significant change to any risk component;
- 6.14.6 not used;
- 6.14.7 where the Supplier has previously Processed Personal Data that does not include Special Category Personal Data, it starts to, or proposes to start to, Process Special Category Personal Data under this Schedule 34;
- 6.14.8 a proposal to change any of the Sites from which any part of the Transitional Services are provided;
- 6.14.9 an ISO/IEC 27001 (at least ISO/IEC 27001:2013) audit report produced in connection with the TS Certification Requirements indicates any non-conformities that put the ISO certification and/or CIMS at risk;

and shall update the TS Required Changes Register and provide the updated TS Required Changes Register to the Authority for review and approval within 10 Working Days after the initial notification or such other timescale as may be agreed with the Authority.

- 6.15 If the Supplier fails to implement a change set out in the TS Required Changes Register by the date agreed with the Authority, such failure shall constitute a material Default and:
 - 6.15.1 the Supplier shall immediately cease using the TS Core Information Management System to Process Authority Data until the Default is remedied, unless directed otherwise by the Authority in writing and then it may only continue to Process Authority Data in accordance with the Authority's written directions; and
 - 6.15.2 where such Default is capable of remedy, such Default shall constitute a TS Security Management Failure and may be notified by either Party to the other Party as a Notifiable Default in accordance with Clause 25 (*Rectification Plan Process*).
- 6.16 The Supplier shall review each Change Request against the TS Security Management Plan to establish whether the documentation would need to be amended should such Change Request be agreed and, where a Change Request would require an amendment to the TS Security Management Plan, the Supplier shall set out any proposed amendments to the documentation in the Impact Assessment associated with such Change Request for

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

consideration and approval by the Authority.

- 6.17 The Supplier shall be solely responsible for the costs associated with developing and updating the TS Security Management Plan and carrying out any remedial action required by the Authority as part of the TS Security Assurance process.

7. TS Certification Requirements

- 7.1 The Supplier shall ensure that, at all times during the TS Term, it is certified as compliant with:

7.1.1 ISO/IEC 27001 (at least ISO/IEC 27001:2013) by a UK Accreditation Service (UKAS)-approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013); and

7.1.2 Cyber Essentials Plus,

and shall provide the Authority with a copy of each such certificate of compliance before the Supplier shall be permitted to use the TS Core Information Management System to receive or Process Authority.

- 7.2 Notwithstanding anything else in this Schedule 34, a TS CIMS Sub-contractor shall be treated for all purposes as a TS Key Sub-contractor.

- 7.3 In addition to the obligations contained in Clause 15, the Supplier must ensure that the Key Sub-contract with each TS CIMS Sub-contractor:

7.3.1 contains obligations no less onerous on the TS Key Sub-contractor than those imposed on the Supplier under this Annex 5 (*TS Security Management*); and

7.3.2 provides for the Authority to perform TS Security Assurance of any part of the TS Core Information Management System that the TS CIMS Sub-contractor provides or operates which is not otherwise subject to TS Security Assurance under this Annex.

- 7.4 The Supplier shall ensure that each TS Higher Risk Sub-contractor is certified as compliant with:

7.4.1 ISO/IEC 27001 (at least ISO/IEC 27001:2013) by a UK Accreditation Service (UKAS)-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013); and

7.4.2 Cyber Essentials Plus,

and shall provide the Authority with a copy of each such certificate of compliance before the TS Higher-Risk Sub-contractor shall be permitted to receive or Process Authority Data.

- 7.5 The Supplier shall ensure that each TS Medium Risk Sub-contractor is

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

certified compliant with:

- 7.5.1 ISO/IEC 27001 (at least 27001:2013) or IASME Assurance Level 2;
and
 - 7.5.2 Cyber Essentials Plus.
- 7.6 The Supplier shall ensure that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data:
- 7.6.1 securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013);
 - 7.6.2 satisfies the Authority that their data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and
 - 7.6.3 maintains an asset register of all Authority supplied information, data and equipment to ensure Authority and assets are returned and/or deleted.
- 7.7 The Supplier shall ensure that the Supplier provides the Authority with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph 7 before the Supplier or the relevant Sub-contractor (as applicable) shall be permitted to carry out the secure destruction of the Authority Data.
- 7.8 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 1 Working Day, if the Supplier or any Sub-contractor ceases to be compliant with the TS Certification Requirements and shall or shall procure that the relevant Sub-contractor shall:
- 7.8.1 immediately cease receiving or Processing Authority Data; and
 - 7.8.2 procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Authority Data in accordance with the TS Baseline Security Requirements.
- 7.9 The Authority may agree to exempt in whole or part the Supplier or any Sub-contractor from the TS Certification Requirements. Any exemption must be in writing to be effective. The Supplier must ensure that the Supplier includes the exemption in the TS Security Management Plan.
- 7.10 From the date specified in the TS Security Management Plan and within 3 Working Days of the end of each subsequent month during the TS Term, the Supplier shall provide the Authority with a written report which provides in appropriate detail the status of relevant Certifications as required by this Paragraph 7 including but not limited to their expiry date and associated activities related to their timely renewal, and any failure to remain compliant which may be tracked through the activities detailed in paragraphs 7.8 and 7.9 above.

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

8. TS Security Testing

8.1 The Supplier shall, at its own cost and expense:

8.1.1 procure testing of the TS Core Information Management System by a CHECK Service Provider (an **"IT Health Check"**):

- (a) prior to it submitting the TS Security Management Plan to the Authority for a TS Security Assurance Decision by the Authority;
- (b) unless otherwise agreed by the Authority, before the Supplier is given permission by the Authority to Process or manage any Authority Data;
- (c) if directed to do so by the Authority; and
- (d) once every 12 months during the TS Term;

8.1.2 conduct weekly vulnerability scanning and assessments of the TS Core Information Management System to the extent that the Supplier is required to conduct such vulnerability scanning and assessments as part of the Existing Security Measures (unless otherwise agreed by the Parties);

8.1.3 conduct an assessment as soon as reasonably practicable following receipt by the Supplier or any of its Sub-contractors of a critical vulnerability alert from a supplier of any software or other component of the TS Core Information Management System to determine whether the vulnerability affects the TS Core Information Management System; and

8.1.4 conduct such other tests as are required by:

- (a) any Remediation Action Plans;
- (b) the ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification requirements;
- (c) the TS Security Management Plan; and
- (d) the Authority following a TS Breach of Security or a significant change to the components or architecture of the TS Core Information Management System,

(each a **"TS Security Test"**).

8.2 The Supplier shall provide the Authority with the results of such TS Security Tests (in a form approved by the Authority in advance) as soon as practicable, and in any case within 7 Working Days, after completion of each TS Security Test.

8.3 In relation to each IT Health Check, the Supplier shall:

8.3.1 agree with the Authority the aim and scope of the IT Health Check;

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- 8.3.2 promptly, and in any case no later than 7 Working Days, following receipt of each IT Health Check report, provide the Authority with a copy of the IT Health Check report;
- 8.3.3 in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall (except where Paragraph 8.3.4 applies)::
- (a) prepare a remedial plan for approval by the Authority (each a **“Remediation Action Plan”**) which sets out in respect of each vulnerability identified in the IT Health Check report:
 - (i) how the vulnerability will be remedied;
 - (ii) unless otherwise agreed in writing between the Authority and the Supplier, the date by which the vulnerability will be remedied, which must be:
 - (A) within 80 Working Days of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “medium”;
 - (B) within 15 Working Days of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “high”;
 - (C) within 5 Working Days of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “critical”;
 - (iii) the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Authority, include a further IT Health Check) to confirm that the vulnerability has been remedied;
 - (b) comply with the Remediation Action Plan; and
 - (c) conduct such further TS Security Tests on the TS Core Information Management System to provide independent evidence that the Supplier has complied with the Remediation Action Plan;

8.3.4 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- [REDACTED]
- 8.4 The Supplier shall design and implement the TS Security Tests so as to minimise the impact on the delivery of the Transitional Services and the date, timing, content and conduct of such TS Security Tests shall be agreed in advance with the Authority. Subject to the Supplier complying with this Paragraph 8.4, if a TS Security Test causes a Service Level Failure in a particular Measurement Period, the Supplier shall be granted relief in respect of such Service Level Failure for that Measurement Period.
- 8.5 The Authority shall be entitled to send a representative to witness the conduct of the TS Security Tests. Without prejudice to the Supplier's obligations under Paragraph 8.3, the Supplier shall provide the Authority with the results of such TS Security Tests (in a form approved by the Authority in advance) as soon as practicable, and in any case no later than 7 Working Days, after completion of each TS Security Test.
- 8.6 The Authority and/or its authorised representatives shall be entitled, at any time and without giving notice to the Supplier, at the Authority's cost, to carry out such tests (including penetration tests) as it may deem necessary in relation to the Transitional Services (but excluding any part of the Transitional Services to the extent such Transitional Services are provided by the Supplier to other customers as well as the Authority), the TS Information Management System and/or the Supplier's compliance with the TS Security Management Plan ("**Authority TS Security Tests**"). The Authority shall take reasonable steps to notify the Supplier prior to carrying out such Authority TS Security Test to the extent that it is reasonably practicable for the Authority to do so taking into account the nature of the Authority TS Security Test.
- 8.7 The Authority shall notify the Supplier of the results of such Authority TS Security Tests after completion of each Authority TS Security Test.
- 8.8 The Authority TS Security Tests shall be designed and implemented so as to minimise their impact on the delivery of the Transitional Services. If an Authority TS Security Test causes a Supplier Non-Performance, the Authority TS Security Test shall be treated as an Authority Cause, except where the root cause of the Supplier Non-Performance was a weakness or vulnerability exposed by the Authority TS Security Test.
- 8.9 Without prejudice to the provisions of Paragraph 8.3.3, where any TS Security Test carried out pursuant to this Paragraph 8 reveals any actual or potential TS Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Authority of any changes to the TS Core Information Management System and/or the TS Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Authority's prior written approval, the Supplier shall implement such changes to the TS Core Information Management System and/or the TS Security Management Plan and repeat the relevant TS Security Tests in accordance with the timetable

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

agreed with the Supplier and Authority or, otherwise, as soon as reasonably possible.

8.10 If the Authority unreasonably withholds its approval to the implementation of any changes proposed by the Supplier to the TS Security Management Plan in accordance with Paragraph 8.8 above, the Supplier shall not be deemed to be in breach of this Schedule 34 to the extent it can be shown that such breach:

8.10.1 has arisen as a direct result of the Authority unreasonably withholding its approval to the implementation of such proposed changes; and

8.10.2 would have been avoided had the Authority given its approval to the implementation of such proposed changes.

8.11 For the avoidance of doubt, where a change to the TS Core Information Management System and/or the TS Security Management Plan is required to remedy non-compliance with the TS Security Management Plan, the TS Baseline Security Requirements and/or any obligation in Schedule 34, the Supplier shall effect such change at its own cost and expense.

8.12 If any repeat TS Security Test carried out pursuant to Paragraph 8.9 reveals an actual or potential TS Breach of Security or weakness exploiting the same root cause failure, such circumstance shall constitute a TS Security Management Failure and may (where it is capable of remedy) be notified by either Party to the other Party as a Notifiable Default in accordance with Clause 25 (*Rectification Plan Process*).

8.13 The Supplier shall, by 31 March of each year during the TS Term, provide to the Authority a letter from its Chief Information Security officer (or equivalent senior officer with responsibility for cyber) confirming that, having made due and careful enquiry:

8.13.1 the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters under this Schedule 34; and

8.13.2 the Supplier is confident that its security and risk mitigation procedures with respect to the Transitional Services remain effective.

8.14 From the date specified in the TS Security Assurance Plan and within 5 Working Days of the end of each subsequent month during the TS Term, the Supplier shall provide the Authority with a written report which provides in appropriate detail the status of vulnerabilities identified through IT Health Checks of the TS Core Information Management System, the elapsed time between the discovery / notification of vulnerabilities their satisfactory remediation, outstanding actions related to mitigation or remediation of public release date of patches.

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

9. Not used**10. Malicious Software**

- 10.1 The Supplier shall install and maintain Anti-Malicious Software on any part of the TS Information Management System which may Process Authority Data and ensure that such Anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the TS Information Management System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the TS Information Management System, to identify, contain the spread of, and minimise the impact of Malicious Software.
- 10.2 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any Losses and to restore the Transitional Services to their desired operating efficiency.
- 10.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 10.2 shall be borne by the Parties as follows:
- 10.3.1 by the Supplier where the Malicious Software originates from:
- (a) the Supplier Software;
 - (b) the Third-Party Software supplied by the Supplier; or
 - (c) the Authority Data whilst the Authority Data is or was under the control of the Supplier,
- unless, in the case of the Authority, the Supplier can demonstrate that such Malicious Software was present in the Authority Data and not quarantined or otherwise identified by the Authority when the Authority provided the Authority Data to the Supplier; and
- 10.3.2 by the Authority where the Malicious Software was present in the Authority Data and not quarantined or otherwise identified by the Authority when the Authority provided the Authority Data to the Supplier.
- 10.4 To the extent that the Supplier is required to provide the same as part of the Existing Services and/or the Existing Security Measures, the Supplier shall (unless otherwise agreed by the Parties) from the date specified in the TS Security Assurance Plan and within 3 Working Days of the end of each subsequent month during the TS Term, provide the Authority with a written report which details the Anti-Malware Software deployment coverage and health based on appropriate metrics including but not limited to compliance with target configuration, positive and false-positive detection rates, and performance.

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

11. TS Breach of Security

- 11.1 If either Party becomes aware of a TS Breach of Security or an attempted TS Breach of Security, it shall notify the other Party in accordance with the security incident management process as set out in the TS Security Management Plan.
- 11.2 The security incident management process set out in the TS Security Management Plan shall, as a minimum, require the Supplier upon becoming aware of a TS Breach of Security or an attempted TS Breach of Security to:
- 11.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Authority which shall be completed within such timescales as the Authority may reasonably require) necessary to:
- (a) minimise the extent of actual or potential harm caused by such TS Breach of Security;
 - (b) remedy such TS Breach of Security to the extent possible and protect the integrity of the TS Information Management System against any such potential or attempted TS Breach of Security;
 - (c) apply a tested mitigation against any such TS Breach of Security or potential or attempted TS Breach of Security and, provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to deliver the Transitional Services so as to meet any TS Performance Level, the Supplier shall be granted relief against the failure to meet such affected TS Performance Level for such period as the Authority, acting reasonably, may specify by written notice to the Supplier; and
 - (d) prevent a further TS Breach of Security or attempted TS Breach of Security in the future exploiting the same root cause failure;
- 11.2.2 as soon as reasonably practicable and, in any event, within 2 Working Days, following the TS Breach of Security or attempted TS Breach of Security, provide to the Authority full details of the TS Breach of Security or attempted TS Breach of Security, including a root cause analysis where required by the Authority.
- 11.3 In the event that any action is taken in response to a TS Breach of Security or attempted TS Breach of Security which occurred as a result of non-compliance of the TS Information Management System and/or the TS Security Management Plan with the TS Baseline Security Requirements and/or this Schedule 34, then such action and any required change to the TS Information Management System and/or TS Security Management Plan shall be completed by the Supplier at no cost to the Authority.
- 11.4 If the Supplier fails to comply with its obligations set out in this Paragraph 11, such failure shall constitute a TS Security Management Failure which may

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

(where such Default is capable of remedy) be notified by either Party to the other Party as a Notifiable Default in accordance with Clause 25 (Rectification Plan Process).

- 11.5 From the date specified in the TS Security Assurance Plan and within 3 Working Days of the end of each subsequent month during the TS Term, the Supplier shall provide the Authority with a written report which details incidents related to TS Breach of Security over time, associated incident record identifiers, problem record identifiers, TS Required Change identifiers, the latest status and next action such that any TS Breach of Security is appropriately tracked and visible through Reporting.

12. Data Processing, Storage, Management and Destruction

- 12.1 The Supplier's obligations in respect of Processing Personal Data and compliance with the Data Protection Legislation are set out in Clause 21.
- 12.2 The Supplier shall only Process Authority Data (that is not Personal Data) in the UK, except where the Authority has given its consent in writing to a transfer of the Authority Data to such other country (including transfers to countries in the European Economic Area) which may be subject to conditions.
- 12.2A The Authority acknowledges and agrees that the Supplier and any of its Sub-contractors, in their capacity as a provider of the Transitional Services under this Schedule 34, may transfer Authority Data (that is not Personal Data) outside of the UK to the European Economic Area in satisfaction of Paragraph 12.2 above and Paragraph 3.2 of Appendix 1 (*TS Baseline Security Requirements*) to the extent it does so in respect of the Existing Services in accordance with the Existing Security Measures and can demonstrate that it has already obtained the Authority's consent to such transfer out of the UK.
- 12.3 In addition to the obligations on the Supplier set out Clause 21 and Paragraph 12.2, the Supplier shall:
- 12.3.1 on demand, provide the Authority with all Authority Data, in an agreed open format, in accordance with the timescales specified in the demand which have been agreed between the Supplier and the Authority for the relevant Authority Data;
 - 12.3.2 have documented processes to guarantee availability of Authority Data in the event of the Supplier ceasing to trade;
 - 12.3.3 securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority other than in relation to Authority Data which is owned or licenced by the Supplier or in respect of which the Parties are either Independent Controllers or Joint Controllers; and
 - 12.3.4 securely destroy all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in this Schedule 34 and, in the absence of any such requirements, as directed by the Authority other than in relation to Authority Data which is owned or licenced by the Supplier or in respect of which the Parties

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

are either Independent Controllers or Joint Controllers.

13. Security Monitoring and Reporting

13.1 The Supplier shall:

- 13.1.1 prepare and submit security reports to the Authority, the frequency and nature of which shall be as detailed and agreed in the TS Security Management Plan;
- 13.1.2 provide evidence of the presence and effectiveness of controls to the Authority upon request as required to meet through-life TS Security Assurance and GovAssure, in a format required by the Authority.

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

APPENDIX 1: TS BASELINE SECURITY REQUIREMENTS**1. Risk Assessments**

- 1.1. The Parties recognise the necessity for risk management and that effective risk management controls are essential to meeting, regulatory, and contractual obligations.
- 1.2. The Supplier shall ensure that:
 - 1.2.1. systems and data are categorised in line with Government Security Classifications and relevant Laws as applicable;
 - 1.2.2. any proposal to change the location in which Authority Data and Authority Systems are stored or Processed will be agreed in advance in accordance with the Change Control Procedure;
 - 1.2.3. any security risks relating to systems and services that are in control of the Supplier and/or Sub-contractors pursuant to the delivery of the Transitional Services are identified and documented;
 - 1.2.4. any risks identified in paragraph 1.2.3 are assessed in accordance with Government risk management practices, Authority risk management practices and together with the Authority Representative and/or relevant Boards to ensure that such risks are understood by identified owners, scored appropriately, and have agreed mitigation and remediation plans, or are otherwise formally accepted by the Authority;
 - 1.2.5. security risk assessments are routinely reviewed and updated upon identifying new security vulnerabilities, including using outside sources for security vulnerability information;
 - 1.2.6. all Supplier Personnel engaged in the delivery, support, or operation of the TS Core Information Management System or who Process Authority Data have knowledge of the Statement of Information Risk Appetite (SIRA) and risk management responsibilities; and
 - 1.2.7. supply chain risks associated with the development, acquisition, maintenance and disposal of systems, system components and services, are assessed and managed including documenting of selected mitigating actions and monitoring and reporting performance against those planned actions.

2. Data Classification and Handling

- 2.1. The Supplier shall ensure that it makes known Government Security Classifications and the classification of, and associated handling requirements for, Authority Data Processed by the TS Information Management System to all Supplier Personnel involved in Processing.
- 2.2. If the provision of the Transitional Services requires the Supplier to Process Authority Data which is classified as:

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- 2.2.1. OFFICIAL-SENSITIVE, the Supplier shall comply with any handling instructions provided with the relevant Authority Data; and/or
 - 2.2.2. SECRET or TOP SECRET, the Supplier shall only do so where it has notified the Authority prior to receipt, or if such prior notification is not possible then immediately upon receipt, of such Authority Data and the Supplier shall implement additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.
- 2.3. In respect of digital and non-digital media used for Processing (including storage) of Authority Data, the Supplier shall:
- 2.3.1. control and restrict access to such media to authorised individuals only;
 - 2.3.2. protect and control such media during transport outside of controlled areas using appropriate security measures; and
 - 2.3.3. sanitise digital media with the strength and integrity commensurate with the classification or sensitivity of the Authority Data prior to disposal, release out of organisational control or release for reuse, in line with published Authority guidance on the topic of secure disposal which can be found at: <https://security-guidance.service.justice.gov.uk/secure-disposal-of-it-public-and-private-cloud/#secure-disposal-of-it---public-and-private-cloud>
- 2.4. The Supplier shall ensure that Authority guidance on data handling and sharing found at: <https://security-guidance.service.justice.gov.uk/data-handling-and-information-sharing-guide/#data-handling-and-information-sharing-guide> is known to and followed by all Supplier Personnel involved in Processing.
- 2.5. The Supplier shall ensure that processes are in use to assist in making information-sharing decisions to ensure data is appropriately protected, and mechanisms exist to secure *ad hoc* exchanges of large digital files with authorised parties in line with the standards, Authority guidance and Good Industry Practice.
- 2.6. The Supplier shall ensure that processes are in place to inventory, document and maintain Documentation of data flows for Authority Data that is resident within the Transitional Services' distributed applications, infrastructure, and system components.
- 2.7. The Supplier shall ensure that media and Authority Data are retained in accordance with applicable statutory, regulatory, and contractual obligations.

3. Location of Authority Data

- 3.1. The Parties recognise the need for the Authority's information to be safeguarded under the UK Data Protection regime or a similar regime. The Supplier must be able to state to the Authority the physical locations in which Authority Data may be Processed (including stored) and managed from, and what legal and regulatory frameworks Authority Data will be subject to at all

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

times.

- 3.2. The Supplier shall and shall procure that its Sub-contractors shall only Process Authority Data in the UK, except where the Authority has given its consent in writing to a transfer of the Authority Data to such other country (including transfers to countries in the European Economic Area) which may be subject to conditions.
- 3.3. The Supplier shall agree any change in location of Processing and administration of Authority Data with the Authority in accordance with the Change Control Procedure, and in accordance with Clause 21 (Protection of Personal Data) if the change relates to the Processing of Personal Data.

4. Data Destruction or Deletion

4.1. The Supplier shall:

- 4.1.1. prior to securely sanitising any Authority Data, or when requested to do so by the Authority, provide the Authority with all Authority Data in an agreed open format;
- 4.1.2. have documented processes to ensure the availability of Authority Data in the event of the Supplier ceasing to trade;
- 4.1.3. securely erase in a manner agreed with the Authority any or all Authority Data held by the Supplier when requested to do so by the Authority;
- 4.1.4. securely destroy in a manner agreed with the Authority all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in this Schedule 34 and, in the absence of any such requirements, as agreed by the Authority; and
- 4.1.5. document and implement processes agreed by the Authority which address the NCSC guidance on secure sanitisation.

5. End User Devices

- 5.1. The Supplier must manage, and must ensure that all Sub-contractors manage, effective security controls on all end-user devices used by the Supplier (and Sub-contractors) on which Authority Data is Processed in accordance with the following requirements:
- 5.1.1. the operating system and any applications that Process or have access to Authority Data must be in current support by the vendor, or the relevant community in the case of Open-Source operating systems or applications;
- 5.1.2. users must authenticate before gaining access;
- 5.1.3. all Authority Data must be encrypted using an encryption tool agreed to by the Authority;

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- 5.1.4. the end-user device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the end-user device is inactive;
 - 5.1.5. the end-user device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Authority Data to facilitate continuous enforcement and reporting on configuration compliance;
 - 5.1.6. the Supplier or Sub-contractor, as applicable, can, without physical access to the end-user device, remove or make inaccessible all Authority Data on the device and prevent any user or group of users from accessing the device;
 - 5.1.7. all end-user devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification issued by a UKAS-approved certification body where the scope of that certification includes the Transitional Services;
 - 5.1.8. the end-user device must utilise anti-malware technologies to detect and eradicate malicious code.
- 5.2. The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance, as they are updated, amended, or replaced on an ongoing basis, as if those recommendations were incorporated as specific obligations under this Schedule 34.
- 5.3. Where there is any conflict between the requirements of this Annex 5 (*TS Security Management*) and the requirements of the NCSC Device Guidance, the requirements of this Annex will take precedence.

6. Encryption

- 6.1. The Supplier must ensure, and must ensure that all Sub-contractors ensure, that:
- 6.1.1. Authority Data is encrypted when stored at any time when no operation is being performed on it;
 - 6.1.2. Authority Data is encrypted when transmitted;
 - 6.1.3. in the implementation of cryptographic protections controls, known public standards and trusted cryptographic technologies are used; and
 - 6.1.4. cryptographic key management controls to protect the confidentiality, integrity, and availability of keys and trust chains are utilised.
- 6.2. Where the Supplier, or a Sub-contractor, cannot encrypt Authority Data the Supplier must:

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- 6.2.1. Immediately inform the Authority of the subset or subsets of Authority Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
 - 6.2.2. provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and
 - 6.2.3. provide such other information as the Authority may require relating to the Authority Data concerned.
- 6.3. The Parties, and, where the Authority requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Authority Data.
- 6.4. Where the Authority and Supplier reach agreement, the Supplier must update the TS Security Management Plan to include:
 - 6.4.1. the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and
 - 6.4.2. the protective measure that the Supplier and/or Sub-contractor will put in place in respect of the unencrypted Authority Data.
- 6.5. Where agreement in accordance with paragraph 6.3 within 35 Working Days of the date on which the Supplier first notified the Authority that it could not encrypt certain Authority Data, either Party may refer the matter to be determined in accordance with the Dispute Resolution Procedure.

7. Personnel Security

- 7.1. All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Transitional Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record.
- 7.2. The Parties shall review the roles and responsibilities of Supplier Personnel who will be involved in the management and/or provision of the Transitional Services in order to enable the Authority to determine the required level of national security vetting clearance per role in accordance with the Cyber and Technical Security Guidance published at <https://security-guidance.service.justice.gov.uk/#cyber-and-technical-security-guidance>.
- 7.3. The Supplier shall not permit Supplier Personnel who fail the security checks required by Paragraph 7.1 and/or fail to meet the clearance requirements of Paragraph 7.2 to be involved in the management and/or provision of the Transitional Services except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Transitional Services.

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- 7.4. The Supplier shall ensure that Supplier Personnel are only granted such access to Authority Data as is necessary to enable the Supplier Personnel to perform their role and to fulfil their responsibilities.
- 7.5. The Supplier shall ensure that Supplier Personnel who no longer require access to Authority Data (e.g. they cease to be employed by the Supplier or any of its Sub-contractors) have their rights to access Authority Data revoked as soon as practicable within at most one Working Day.
- 7.6. The Supplier shall ensure that processes are in place to govern and manage data access controls upon the termination of individual employment of Supplier Personnel.
- 7.7. The Supplier shall ensure that Supplier Personnel that have access to the Sites, the TS IT Environment or the Authority Data receive regular training on security awareness that reflects the degree of access those individuals have to the Sites, the TS IT Environment or the Authority Data.
- 7.8. The Supplier shall ensure that the training provided to Supplier Staff under Paragraph 7.7 includes training on the identification and reporting of fraudulent communications intended to induce individuals to disclose Personal Data or any other information that could be used, including in combination with other Personal Data or information, or with other techniques, to facilitate unauthorised access to the Sites, the TS IT Environment or the Authority Data ("phishing").
- 7.9. The Supplier shall implement and maintain separation of duties where appropriate, including to prevent potential inappropriate activity.
- 7.10. The Supplier shall ensure all Supplier Personnel to apply cybersecurity and privacy principles in their daily work.

8. Identity, Authentication and Access Control

- 8.1. The Supplier shall operate an identification and access management control regime to ensure:
- 8.1.1. all users, administrators and processes, including any third-party users and processes, are uniquely identified and centrally authenticated, authorised, and audited when accessing or administering the Transitional Services;
 - 8.1.2. all persons who access the Sites are identified and authenticated before they are allowed access to the Sites;
 - 8.1.3. all devices are uniquely identified, and centrally authenticated, authorised, and audited before establishing a connection, which must be cryptographically based and replay-resistant;
 - 8.1.4. mechanisms are in place at all times to identify and authenticate any third-party systems and services;
 - 8.1.5. mechanisms are in place at all times to securely manage authenticators for users and devices; and

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- 8.1.6. identifiers are not shared or re-used between environments.
- 8.2. The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) when allowing or configuring access to the Supplier TS System and Sites so that such access is only to those parts of the Sites and the Supplier TS System that the relevant Supplier Personnel require to accomplish assigned tasks.
- 8.3. The Supplier shall ensure that role-based access control (RBAC) policy over users and resources applies need-to-know and fine-grained access control, enforcing principles of least privilege.
- 8.4. The Supplier shall retain records of access to the Sites and to the Supplier TS System and shall make such records available to the Authority on request.
- 8.5. The Supplier shall enforce multi-factor authentication (MFA) where published guidance demands or recommends it and for remote network access, third party systems, applications and/or services, and/or for non-console privileged access to systems.
- 8.6. The Supplier shall pro-actively govern account management of all accounts including user, privileged user, and non-user accounts, utilising registration and de-registration processes to govern the assignment of user rights.
- 8.7. The Supplier shall periodically (at least every 3 months) review the privileges assigned to user and non-user accounts to validate the need for such privileges, reassign or remove unnecessary privileges as necessary, and provide appropriate associated reporting to the Authority illustrating control over access, privileged access, and granted privileges.

9. Audit and Protective Monitoring

The following obligations in this Paragraph 9 shall (unless otherwise agreed by the Parties) only apply to the extent that they form part of the Existing Services and/or the Existing Security Measures:

- 9.1. The Supplier shall collect audit records which relate to security Events in the TS Core Information Management System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness, such audit records shall (as a minimum) include regular reports and alerts setting out details of access by users of the TS Core Information Management System, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data .
- 9.2. In addition to any requirement in Clause 37.3, the Supplier shall:
- 9.2.1. Implement audit and monitoring of the TS Core Information Management System sufficient to comply with any applicable Relevant Requirements and to prevent or detect any Prohibited Act;
- 9.2.2. Keep sufficient records to demonstrate compliance with the requirements of Paragraph 9.2.1 to the Authority; and

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- 9.2.3. Make those records and any documents describing the audit and monitoring undertaken to the Authority on request.
- 9.3. The Parties shall work together to establish any additional audit and monitoring requirements for the TS Core Information Management System.
- 9.4. The retention periods for audit records and event logs must be agreed with the Authority and documented in the TS Security Management Plan.
- 9.5. The Supplier shall detect and respond to indicators of system or account compromise, indicators of unauthorised exfiltration of non-public information, and other potentially malicious activities.
- 9.6. The Supplier TS System must be configured by the Supplier to produce audit records to, at a minimum, generate audit records for system Events, authorisation Events, failure or error-related Events, and all security operations and functions.
- 9.7. The Supplier TS System must be configured by the Supplier such that audit records contain sufficient information to meet published Authority Cyber and Technical Security Guidance found at: <https://security-guidance.service.justice.gov.uk/#cyber-and-technical-security-guidance> and:
- [REDACTED]
- 9.8. The Supplier shall protect the confidentiality, integrity, and availability of Event logs within its control by:
- 9.8.1. managing sufficient storage capacity to reduce the likelihood that capacity is exceeded as a consequence of the Event logs;
- 9.8.2. alerting the Authority in the event of a log processing failure;
- 9.8.3. protecting logs from unauthorised access, modification, or deletion; and
- 9.8.4. configuring systems to use an authoritative time source synchronised with the Master Time Reference (as that term is used in Annex 2 (*TS Service Descriptions*) to Schedule 34 to generate time stamps for logs.
- 9.9. The Supplier shall keep sufficient records related to audit and monitoring, including in accordance with Schedule 24 (Reports and Records Provisions), for compliance with the requirements of Paragraph 9.2.1 through regular reporting to the Authority.

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

9.10. The Supplier shall provide to the Authority audit records generated by or pertaining to access to Authority Systems, such that the Authority may perform direct analysis of recorded Events; such records to be provided to the Authority on request or through automated log transmission mechanism(s).

10. Security Operations

10.1. The Supplier shall implement operational security controls to:

10.1.1. define and deliver capabilities supporting the Authority based on Good Industry Practice to meet the Authority's service needs; and

10.1.2. utilise and collaborate with the capabilities available through the Authority's security operations centre.

11. Threat Management

11.1. The Supplier shall monitor threat intelligence sources as part of day to day operations related to the security of the Transitional Services, and notify the Authority of any threat intelligence information that may influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.

11.2. The Supplier shall develop and maintain a documented understanding of potential attack vectors that could be used to attack the TS Core Information Management System through the Risk Assessment contained in the TS Security Management Plan.

11.3. The Supplier shall maintain situational awareness of evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the recommendation and subsequent implementation of preventative and compensating controls.

12. Information Assurance

12.1. The Supplier shall:

12.1.1. facilitate the implementation and use of data privacy impact assessments and relevant authorisation controls, including use of the Authority's privacy assessment and authorisation controls;

12.1.2. formally assess the cybersecurity and privacy controls of the Supplier TS System and TS Licensed Software periodically, to determine the extent to which the controls are implemented correctly, operating as intended, producing the desired outcomes and meeting expected requirements;

12.1.3. maintain in the Virtual Library key architectural TS Documentation and information on each critical system, application or service. Such TS Documentation shall utilise Good Industry Practice and shall be suitable for influencing inputs, entities, systems, applications and processes, and for use as Records of the relevant data and its origins;

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- 12.1.4. evaluate the design, implementation and effectiveness of technical cybersecurity and privacy controls relating to the Transitional Services; and
- 12.1.5. ensure systems, projects and services are formally authorised by the Authority prior to being implemented by the Supplier in the TS IT Environment and/or Operating Environment.

13. Physical and Environmental Security

13.1. Where physical and environmental security is in the control of the Supplier or Sub-Contractor, the Transitional Supplier shall ensure that:

- 13.1.1. mechanisms are in place to facilitate the operation of proportionate physical and environmental protection controls; and
- 13.1.2. physical access control mechanisms are in place to maintain a current list of Supplier Personnel and personnel of the Authority with authorised access to facilities (except for those areas within the facility officially designated as publicly accessible).

14. Project and Resource Management

14.1. The Supplier shall ensure that TS Changes, TS Operational Changes and TS Service Changes are impact-assessed from a security perspective, to ensure that vulnerabilities are not introduced to the estate and that the TS Security Management Plan can be updated in a timely manner to accommodate changes which impact the TS Security Management Plan.

14.2. The Supplier shall operate effective knowledge management for all Supplier Personnel responsible for cybersecurity and privacy, regarding knowledge of the Authority's and the Service Recipients' operational needs as required for effective security management.

15. Security Awareness and Training

15.1. The Supplier shall facilitate the implementation of security workforce development and awareness controls to:

- 15.1.1. provide all Supplier Personnel with appropriate security awareness education and training that is relevant for their job function;
- 15.1.2. provide role-based security-related training before authorising access to the system or performing assigned duties, when required by system changes, and annually thereafter; and
- 15.1.3. document, retain and monitor individual training activities, including basic security awareness training, ongoing awareness training and specific-system training.

16. Vulnerability and Patch Management

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- 16.1. The Parties acknowledge that vulnerabilities in the TS Information Management System may be discovered which unless mitigated will present an unacceptable risk to the Authority Data, and that the implementation and monitoring of effective vulnerability management controls are critical to protecting confidentiality, integrity and availability.
- 16.2. The Supplier shall ensure that controls are implemented in the TS Information Management System to ensure that vulnerabilities are properly identified, tracked, and remediated during the Term.
- 16.3. The Supplier shall ensure that mechanisms are in place to detect vulnerabilities and configuration errors in the TS Information Management System by recurring vulnerability scanning of systems and web applications.
- 16.4. The severity of vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the method described in the TS Security Management Plan and using the appropriate vulnerability scoring systems including:
- 16.4.1. the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'Critical', 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST at <http://nvd.nist.gov/cvss.cfm>); and
- 16.4.2. Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.
- 16.5. Subject to Paragraph 16.6, the Supplier shall procure the application of security patches to vulnerabilities in the TS Information Management System within:
- 16.5.1. seven (7) days after the public release of patches for those vulnerabilities categorised as 'Critical';
- 16.5.2. thirty (30) days after the public release of patches for those vulnerabilities categorised as 'Important' and
- 16.5.3. sixty (60) days after the public release of patches for those vulnerabilities categorised as "Other".
- 16.6. The Supplier shall ensure all patches planned for release are tested in accordance with the release management process agreed with the Authority, and deployed in accordance with the Change Management Process.
- 16.7. The timescales for applying patches to vulnerabilities in the TS Information Management System set out in Paragraph 16.5 shall be extended by the Authority where:
- 16.7.1. the Supplier can demonstrate that a vulnerability in the TS Information Management System is not exploitable within the context of the Transitional Services (e.g. because it resides in a TS Software

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

component which is not involved in running in the Transitional Services) provided such vulnerabilities shall be remedied by the Transitional Supplier within the timescales set out in Paragraph 16.5 if the vulnerability becomes exploitable within the context of the Transitional Services;

- 16.7.2. the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Transitional Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or
 - 16.7.3. the Authority agree a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the TS Security Management Plan.
- 16.8. The TS Security Management Plan shall include provisions for major version upgrades of all COTS Software to be kept up-to-date, such that all COTS Software shall always be in mainstream support throughout the TS Term unless otherwise agreed by the Authority in writing. All COTS Software should be no more than N-1 versions behind the latest software release.
- 16.9. The Supplier shall not release any software (including update) to the TS IT Environment and/or Operating Environment without evidence of a current vulnerability scan, associated mitigations, or documented exemption(s) approved by the Authority.
- 16.10. In regard to the TS Security Tests, the Supplier shall:
- 16.10.1. specify in the TS Security Management Plan the scope of the TS Information Management System to be CHECK tested;
 - 16.10.2. at its own cost and expense, procure and conduct tests to the TS Information Management System in accordance with the TS Security Management Plan;
 - 16.10.3. at its own cost and expense (unless otherwise agreed), procure and conduct such other security tests as may be reasonably required to provide the necessary assurances that controls are in place; and
 - 16.10.4. provide the Authority with the full results of the tests conducted under Sub-paragraphs 16.10.2 and/or 16.10.3, promptly following the completion of each such test.
- 16.11. The frequency of the tests required under Sub-Paragraph 16.10.2 shall be once per Contract Year or as may be otherwise more frequently specified in the TS Security Management Plan.
- 16.12. To the extent the Supplier is required to provide such reports as part of the Existing Services and/or the Existing Security Measures, the Supplier shall report to the Authority within the performance management report provided in

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

accordance with paragraph 5 of Annex 3 (*TS Performance Levels*) (or such other monthly report as may be agreed by the Authority from time to time):

- 16.12.1. patched and outstanding vulnerabilities in the TS Information Management System (to the extent that the TS Information Management System is within the control of the Transitional Supplier);
- 16.12.2. any elapsed time from the public release date of patches to the patches being applied;
- 16.12.3. either the date of application or, for outstanding vulnerabilities, the planned date; and
- 16.12.4. proposed interim mitigation measures for vulnerabilities in the managed environment which are known to be exploitable, where a security patch is not immediately available.

17. Asset Management

17.1. The Supplier must manage, and ensure that all Sub-contractors manage, all Authority Assets such that:

- 17.1.1. Authority Assets are inventoried in the ITSM Toolset to accurately reflect the current systems, applications, and services;
- 17.1.2. asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organisation level;
- 17.1.3. network and solution architecture diagrams are maintained, with sufficient detail to assess the security and reflect the current architecture;
- 17.1.4. sanctions that require the removal and prohibition of certain technology services and/or equipment that are designated as threats by a statutory or regulatory body are implemented; and
- 17.1.5. proper decommissioning processes for systems, applications and services are used, so that Authority Data is properly transitioned to new systems or archived in accordance with applicable organisational standards, as well as statutory, regulatory and contractual obligations, and that information is prevented from being recovered from decommissioned components following secure disposal, destruction, or repurposing.

18. Configuration Management

18.1. The Supplier shall ensure:

- 18.1.1. configuration management controls are in use;
- 18.1.2. develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards;

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- 18.1.3. configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services;
- 18.1.4. restrict the ability of non-privileged users to install unauthorised software; and
- 18.1.5. obtain, protect, maintain, update, and distribute administrator documentation that describe:
- 18.1.6. secure configuration, installation and operation; and
- 18.1.7. effective use and maintenance of security features/functions.

19. Maintenance

19.1. The Supplier must ensure:

- 19.1.1. mechanisms are in place to develop, disseminate, review and update procedures to facilitate the implementation and validation of maintenance controls related to the TS Core Information Management System;
- 19.1.2. processes are in place to protect the authenticity, confidentiality, integrity, and availability of assets during maintenance activities impacting the TS Core Information Management System;
- 19.1.3. mechanisms are in place to authorise, monitor, and control all maintenance and diagnostic activities, including any remote maintenance, and including any associated transfer and storage;
- 19.1.4. proper physical security and configuration control over Authority Assets awaiting service or repair; and
- 19.1.5. the use of system maintenance tools within the TS Core Information Management System is controlled and monitored by the Supplier.

20. Security Incident Response

20.1. The Supplier shall:

- 20.1.1. implement and govern processes and TS Documentation to facilitate a response capability for Security Incidents, including to meet the TS Performance Levels;
- 20.1.2. respond to all Security Incidents as raised to the Supplier by the Authority;
- 20.1.3. put in place the capabilities to identify and pro-actively manage the estate against Security Incidents;
- 20.1.4. document, monitor and report the status of Security Incidents to the Authority all the way through to Resolution (as defined in Annex 3 (*TS Performance Levels*) to Schedule 34) of each Security Incident;

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- 20.1.5. ensure a viable and current Security Incident response process is documented in the TS Security Management Plan covering the intake of Security Incident reporting, analysis, eradication and recovery;
- 20.1.6. define specific indicators of compromise to identify the signs of potential cybersecurity Events;
- 20.1.7. ensure an integrated (virtual) team of cybersecurity, IT, and business function representatives appropriate and proportional to the purposes of the Security Incident response function and appropriate to the Transitional Services is defined and maintained in the TS Security Management Plan;
- 20.1.8. ensure Supplier Personnel are provided with guidance and/or training by the Supplier in their Security Incident response roles and responsibilities;
- 20.1.9. formally test Security Incident response capabilities periodically through realistic exercises to determine the operational effectiveness of those capabilities;
- 20.1.10. document, monitor and report the status of Security Incidents to internal stakeholders, affected third parties and where, required to do so by Law, regulatory authorities, through to Resolution (as defined in Annex 3 (*TS Performance Levels*) to Schedule 34) of the Security Incident;
- 20.1.11. ensure documented processes agreed by the Authority are in place to facilitate a rapid and secure response to any security investigation undertaken by the Authority;
- 20.1.12. ensure that the integrity of data which might subsequently be relied upon in Court shall be maintained throughout a forensic investigation process; and
- 20.1.13. ensure documented processes are defined and followed by the Supplier so that lessons are learned from analysing and resolving Security Incidents to reduce the likelihood or impact of future Security Incidents.

21. Compliance**21.1. The Supplier must:**

- 21.1.1. facilitate the identification and implementation of relevant statutory, regulatory, and contractual controls;
- 21.1.2. operate a security and privacy controls oversight function that reports to its executive leadership;
- 21.1.3. ensure its managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate security policies, standards and other applicable requirements;

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- 21.1.4. maintain all relevant certifications with appropriate accredited bodies; and
- 21.1.5. support the Authority in meeting legal and regulatory obligations, including data protection impact assessments (DPIAs), Requests for Information and subject access requests (SARs), Departmental Security Health Check (DSHC) and other authorised compliance audits.

22. Secure Engineering and Architecture

22.1. The Supplier shall utilise Good Industry Practice cybersecurity and privacy approaches and principles that address risk to organisational operations, assets, individuals, and other organisations in the specification, design, development, implementation and modification of systems and services in accordance with:

- 22.1.1. Cyber and Technical Security Guidance <https://security-guidance.service.justice.gov.uk/#cyber-and-technical-security-guidance>;
- 22.1.2. HMG Secure by Design <https://www.security.gov.uk/guidance/secure-by-design/>;
- 22.1.3. NCSC guidance which can be found at: <https://www.ncsc.gov.uk/section/advice-guidance/all-topics>;
- 22.1.4. the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main>;
- 22.1.5. the NCSC "Bulk Data Principles", a copy of which can be found at <https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main>; and
- 22.1.6. the NCSC "Cloud Security Principles", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles> and which are summarised below:
 - (a) "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;
 - (b) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;
 - (c) "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- (d) "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Transitional Services and information within it;
- (e) "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Transitional Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;
- (f) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Personnel have access to Authority Data and/or the Authority System that those personnel be subject to appropriate security screening and regular security training;
- (g) "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Transitional Services be designed and developed to identify and mitigate threats to their security;
- (h) "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Sub-contractors and other suppliers;
- (i) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Authority to securely manage the Authority's use of the Transitional Services;
- (j) "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;
- (k) "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Transitional Services should be identified and appropriately defended;
- (l) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;
- (m) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Authority with the audit records it needs to monitor

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

access to the Service and the Authority Data held by the Supplier and/or its Sub-contractors; and

- (n) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Personnel on the safe and secure use of the TS Information Management System.

22.2. The Supplier shall ensure that all critical system clocks shall be synchronised with the Master Time Reference.

22.3. To the extent that the Supplier is responsible for solution design, such design shall take account of all controls (e.g. segregation) necessary for the protection of Authority Data, and the Transitional Services, in accordance with the SIRA, from vulnerabilities including those which may arise during development, testing and Release Management.

22.4. The Supplier shall notify the Authority of any insufficiency (or risk of insufficiency) of the controls required under Paragraph 22.3.

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

APPENDIX 2: TS SUB-CONTRACTOR SECURITY REQUIREMENTS**1 Application of Appendix 2**

1.1 This Appendix 2 applies to all Sub-contractors that Process Authority Data

1.2 The Supplier must:

- (a) ensure that those Sub-contractors comply with the provisions of this Appendix 2;
- (b) keep sufficient records to demonstrate that compliance to the Authority; and
- (c) ensure that its Implementation Plan includes deliverable items and dates that relate to the design, implementation and management of any systems used by Sub-contractors to Process Authority Data.

2 Designing and managing secure solutions

2.1 The Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a NCSC Certified Professional certification (<https://www.ncsc.gov.uk/articles/cesg-certification-ia-professionals-and-guidance-certification-ia-professionals-documents>) for all bespoke or complex components.

2.2 The Sub-contractor shall implement their solution(s) to mitigate the security risks in accordance with;

- (a) NCSC's Cyber Security Design Principles
<https://www.ncsc.gov.uk/collection/cyber-security-design-principles>;
and
- (b) HMG Secure by Design
<https://www.security.gov.uk/guidance/secure-by-design/>

2.3 The Sub-contractor must (where applicable to the service being provided) assess their systems against the HMG Secure by Design Principles <https://www.security.gov.uk/guidance/secure-by-design/principles/> at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-contractor must document that assessment and make that documentation available to the Authority and/or the Supplier on the Authority's request.

3 Data Processing, Storage, Management and Destruction

3.1 The Supplier shall ensure that Authority Data is protected and Processed in a secure manner. To achieve this objective, the Authority Data shall only be Processed within the United Kingdom subject to Paragraph 12 of Annex 5. The Supplier must align with UK Data Protection Legislation, Cyber and Technical Security Guidance <https://security-guidance.service.justice.gov.uk/#cyber-and-technical-security-guidance>, NCSC Cyber Assessment Framework Guidance, and all NCSC guidance on

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Cyber Security to ensure the security and protection of the Authority Data. In addition, appropriate measures must be put in place to prevent unauthorised access, use, or disclosure of the Authority Data. The Supplier shall agree under the Change Control Procedure, any change in location of Processing and / or administration of Authority Data (in accordance with Clause 21 (Protection of Personal Data) if the TS Change relates to the Processing of Personal Data).

3.2 The Sub-contractor must, when requested to do so by the Authority (in respect of the Authority Data):

- (a) securely destroy Authority Data only on Sites which are included within the scope of an existing ISO/IEC 27001 certification;
- (b) satisfy the Authority that their data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and
- (c) maintain an asset register of all Authority supplied information, data and equipment to ensure Authority assets are returned and/or deleted.

4 Personnel Security

4.1 The Sub-contractor must perform appropriate checks on their staff before they may participate in the provision and or management of the Transitional Services. Those checks must include all pre-employment checks required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record. The HMG Baseline Personnel Security Standard can be found at:
<https://www.gov.uk/government/publications/government-baseline-personnel-security-standard>.

4.2 The Sub-contractor must, if the Authority requires, at any time, ensure that one or more of the Sub-contractor's staff obtains Security Check clearance in order to Process Authority Data containing Personal Data above certain volumes specified by the Authority, or containing Special Category Personal Data.

4.3 Any Sub-contractor staff who will, when performing the Transitional Services, have access to a person under the age of 18 years must undergo Disclosure and Barring Service (DBS) checks.

5 End User Devices

5.1 The Supplier must manage, and must ensure that all Sub-contractors manage, all end-user devices used by the Supplier on which Authority Data is Processed in accordance with the following requirements:

- a) the operating system and any applications that Process or have access to Authority Data must be in current support by the vendor,

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

or the relevant community in the case of Open Source operating systems or applications;

- b) users must authenticate before gaining access;
 - c) all Authority Data must be encrypted using an encryption tool agreed to by the Authority (in respect of the Authority Data);
 - d) the end-user device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the end-user device is inactive;
 - e) the end user device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Authority Data to facilitate continuous enforcement and reporting on configuration compliance;
 - f) the Supplier or Sub-contractor, as applicable, can, without physical access to the end-user device, remove or make inaccessible all Authority Data on the device and prevent any user or group of users from accessing the device;
 - g) all end-user devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification issued by a UKAS-approved certification body, where the scope of that certification includes the Transitional Services provided in relation to the contract.
- (a) mechanisms are in in place at all times to utilise anti-malware technologies to detect and eradicate malicious code.
- 5.2 The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance, as they are updated, amended or replaced on an ongoing basis, as if those recommendations were incorporated as specific obligations under this Schedule 34.
- 5.3 Where there is any conflict between the requirements of this Annex 5 (*TS Security Management*), and the requirements of the NCSC Device Guidance, the requirements of this Annex will take precedence.
- 6 Cryptographic Protections**
- 6.1 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that Authority Data is encrypted:
- (a) when stored at any time when no operation is being performed on it; and
 - (b) when transmitted.
- 6.2 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that it shall:

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- a) in the implementation of cryptographic protections controls, use known public standards and trusted cryptographic technologies; and
 - b) utilise cryptographic key management controls to protect the confidentiality, integrity, and availability of keys and trust chains.
- 6.3 Where the Supplier, or a Sub-contractor, cannot encrypt Authority Data the Supplier must:
- (a) immediately inform the Authority of the subset or subsets of Authority Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
 - (b) provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and
 - (c) provide the Authority with such information relating to the Authority Data concerned, the reasons why that Authority Data cannot be encrypted and the proposed protective measures as the Authority (in respect of the Authority Data) may require.
- 6.4 The Authority, the Supplier, and, where the Authority requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Authority Data.
- 6.5 Where the Authority and/or the Supplier reach agreement, the Supplier must update the TS Security Management Plan to include:
- (a) the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and
 - (b) the protective measure that the Supplier and/or Sub-contractor will put in place in respect of the unencrypted Authority Data.
- 6.6 Where agreement in accordance with paragraph 6.4 is not reached within 35 Working Days of the date on which the Supplier first notified the Authority that it could not encrypt certain Authority Data, either party may refer the matter to be determined in accordance with the Dispute Resolution Procedure.
- 7 Patching and Vulnerability Scanning**
- 7.1 The Sub-contractor must proactively monitor supplier vulnerability websites and ensure all necessary patches and upgrades are applied to maintain security, integrity and availability in accordance with the Patch Management Guide (<https://security-guidance.service.justice.gov.uk/patch-management-guide/#patch-management-guide>), and the NCSC Cloud Security Principles.
- 8 Third Party Sub-contractors**
- 8.1 The Sub-contractor must not transmit or disseminate the Authority Data to any other person unless specifically authorised by the Authority. Such

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

authorisation must be in writing to be effective and may be subject to conditions.

- 8.2 The Sub-contractor must not, when performing any part of the Transitional Services, use any software to Process the Authority Data where the licence terms of that software purport to grant the licensor rights to Process the Authority Data greater than those rights strictly necessary for the use of the software

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

APPENDIX 3: TS SECURITY MANAGEMENT PLAN TEMPLATE**TS Security Management Plan Template****[Project/Service and Supplier Name]****1 Executive Summary**

<This section should contain a brief summary of the business context of the system, any key IA controls, the assurance work done, any off-shoring considerations and any significant residual risks that need acceptance.>

2. System Description**2.1 Background**

< A short description of the project/product/system. Describe its purpose, functionality, aim and scope.>

2.2 Organisational Ownership/Structure

<Who owns the system and operates the system and the organisational governance structure. This should include how any ongoing security management is integrated into the project governance e.g. how a Security Working Group reports to the Enterprise Architecture Board.>

2.3 Information assets and flows

<The information assets processed by the system which should include a simple high level diagram on one page. Include a list of the type and volumes of data that will be processed, managed and stored within the Supplier TS System. If personal data, please include the fields used such as name, address, department DOB, NI number etc.>

2.4 System Architecture

<A description of the physical system architecture, to include the system management. A diagram will be needed here>

2.5 Users

<A brief description of the system users, to include HMG users as well as any service provider users and system managers. If relevant, security clearance level requirements should be included.>

2.6 Locations

<Where the data assets are stored and managed from. If any locations hold independent security certifications (e.g. ISO27001 (at least ISO/IEC 27001:2013) these should be noted. Any off-shoring considerations should be detailed.>

2.7 Test and Development Systems

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

<Include information about any test and development systems, their locations and whether they contain live system data.>

2.8 Key roles and responsibilities

<A brief description of the lead security roles such as that of the SIRO, IAO, Security manager >

3. Risk Assessment

3.1 Assurance Scope

<This section describes the scope of the Assurance for the system. The scope of the assurance assessment should be clearly indicated, with components of the architecture upon which reliance is placed but assurance will not be done clearly shown e.g. a cloud hosting service. A logical diagram should be used along with a brief description of the components.>

3.2 Risk appetite

<A risk appetite should be agreed with the SRO and included here.>

3.3 Business impact assessment

< A description of the information assets and the impact of their loss or corruption (e.g. large amounts of Official Sensitive personal data the loss of which would be severely damaging to individuals, embarrassing to HMG, and make HMG liable to ICO investigations) in business terms should be included. This section should cover the impact on loss of confidentiality, integrity and availability of the assets. The format of this assessment may be dependent on the risk assessment method chosen.>

3.4 Risk assessment

<The content of this section will depend on the risk assessment methodology chosen and should contain the output of the formal information risk assessment in a prioritised list using business language. Experts on the system and business process should have been involved in the risk assessment to ensure the formal risk methodology used has not missed out any risks. The example table below should be used as the format to identify the risks and document the controls used to mitigate those risks. >

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R1	Internet attackers could hack the system.	Medium	The service systems are exposed to the internet via the web portal.	C1: Internet-facing firewalls C2: Internet-facing IP whitelist	Very low

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
				C3: System hardening C4: Protective monitoring C5: Application access control C16: Anti-virus for incoming files C54: Files deleted when processed C59: Removal of departmental identifier	
R2	Remote attackers could intercept or disrupt information crossing the internet.	Medium	File sharing with organisations across the internet.	C9: TLS communications C10: PGP file-sharing	Very low
R3	Internal users could maliciously or accidentally alter bank details.	Medium-High	Users bank details can be altered as part of the normal business function.	C12. System administrators hold SC clearance. C13. All changes to user information are logged and audited. C14. Letters are automatically sent to users' home addresses when	Low

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
				bank details are altered. C15. Staff awareness training	

3.5 Controls

<The controls listed above to mitigate the risks identified should be detailed. There shall be a description of each control, further information and configuration details where relevant, and an assessment of the implementation status of, and assurance in, the control. A sample layout is included below.>

ID	Control title	Control description	Further information and assurance status
C1	Internet-facing firewalls	Internet-facing firewalls are in place between the internet and the system', which restrict access from the internet to the required ports only.	Assured via ITHC firewall rule check
C2	Internet-facing IP whitelist	An IP whitelist is in place for all access from the internet.	Assured via ITHC
C15	Staff awareness training	All staff must undertake annual security awareness training and this process is audited and monitored by line managers.	Assured as part of ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification

3.6 Residual risks and actions

<A summary of the residual risks which are likely to be above the risk appetite stated after all controls have been applied and verified should be listed with actions and timescales included.>

4. In-service controls

< This section should describe the controls relating to the information lifecycle, including development, testing, in-service, termination and on-going risk management and assurance. Details of any formal assurance requirements specified in the contract such as security CHECK testing or maintained ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification should be included. This section should include at least:

- (a) information risk management and timescales and triggers for a review;*
- (b) contractual patching requirements and timescales for the different priorities of patch;*
- (c) protective monitoring arrangements to include how anomalous behaviour is identified and acted upon as well as how logging and auditing of user activity is done;*
- (d) configuration and change management;*
- (e) incident management;*
- (f) vulnerability management;*
- (g) user access management; and*
- (h) data sanitisation and disposal.>*

5. Security Operating Procedures (SyOPs)

< If needed any SyOps requirements should be included and referenced here.>

6. Major Hardware and Software and end of support dates

< This should be a table which lists the end of support dates for hardware and software products and components. An example table is shown below.>

Name	Version	End of mainstream Support/Extended Support	Notes/RAG Status
Server Host	HP XXXX	Feb 2020/ March 2022	

7. Incident Management Process

<The suppliers' process, as agreed with the Authority, should be included here. It must as a minimum include the protocol for how and when incidents will be reported to the Authority and the process that will be undertaken to mitigate the incidents and investigate the root cause.>

8. Security Requirements for User Organisations

ANNEX 5 (TS SECURITY MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

<Any security requirements for connecting organisations or departments should be included or referenced here.>

9. TS Required Changes Register

<The table below shows the headings for the TS Required Changes Register which should be maintained and used to update the contents of this document at least annually.>

Ref	Section	Change	Agreed With	Date agreed	Documentation update	Status
1	6.4	A new Third Party supplier XXXX will be performing the print capability.	Authority name	11/11/2018	Jul-2019	Open

10. Sub-contractors

<This should include a table which shows for each Sub-contractor their name, the function that they are performing, the data and data volume being processed, the location, and their certification status>

11. Appendix A. ISO/IEC 27001 (at least ISO/IEC 27001:2013) and/or Cyber Essential Plus certificates

<Any certifications relied upon should have their certificates included>

12. Appendix B. Cloud Security Principles assessment

<A spreadsheet may be attached>

13. Appendix C. Protecting Bulk Data assessment if required by the Authority

<A spreadsheet may be attached>

14. Appendix D. Latest ITHC report and Remediation Action Plan

ANNEX 7 (AUTHORITY TS RESPONSIBILITIES) to SCHEDULE 34

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

ANNEX 7

AUTHORITY TS RESPONSIBILITIES

ANNEX 7 (AUTHORITY TS RESPONSIBILITIES) to SCHEDULE 34

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

1 INTRODUCTION

- 1.1 In addition to the Authority Responsibilities set out in Schedule 7 (*Authority Responsibilities*), the responsibilities of the Authority set out in Paragraph 2 of this Annex shall also apply for the duration of the TS Term and constitute Authority Responsibilities under this Contract.
- 1.2 The responsibilities specified within this Annex shall be provided to the Supplier free of charge, unless otherwise agreed between the Parties.

2 AUTHORITY OBLIGATIONS

ID	Relevant Document	Authority Responsibility
AO-01	Schedule 34	The Authority shall use its reasonable endeavours to notify the Supplier of any Laws which are specific to the Authority and which the Supplier cannot reasonably be expected to be aware of but which the Supplier will be required to comply with when providing the Transitional Services.

ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Annex 8

SUPPLIER TS SOLUTION

ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

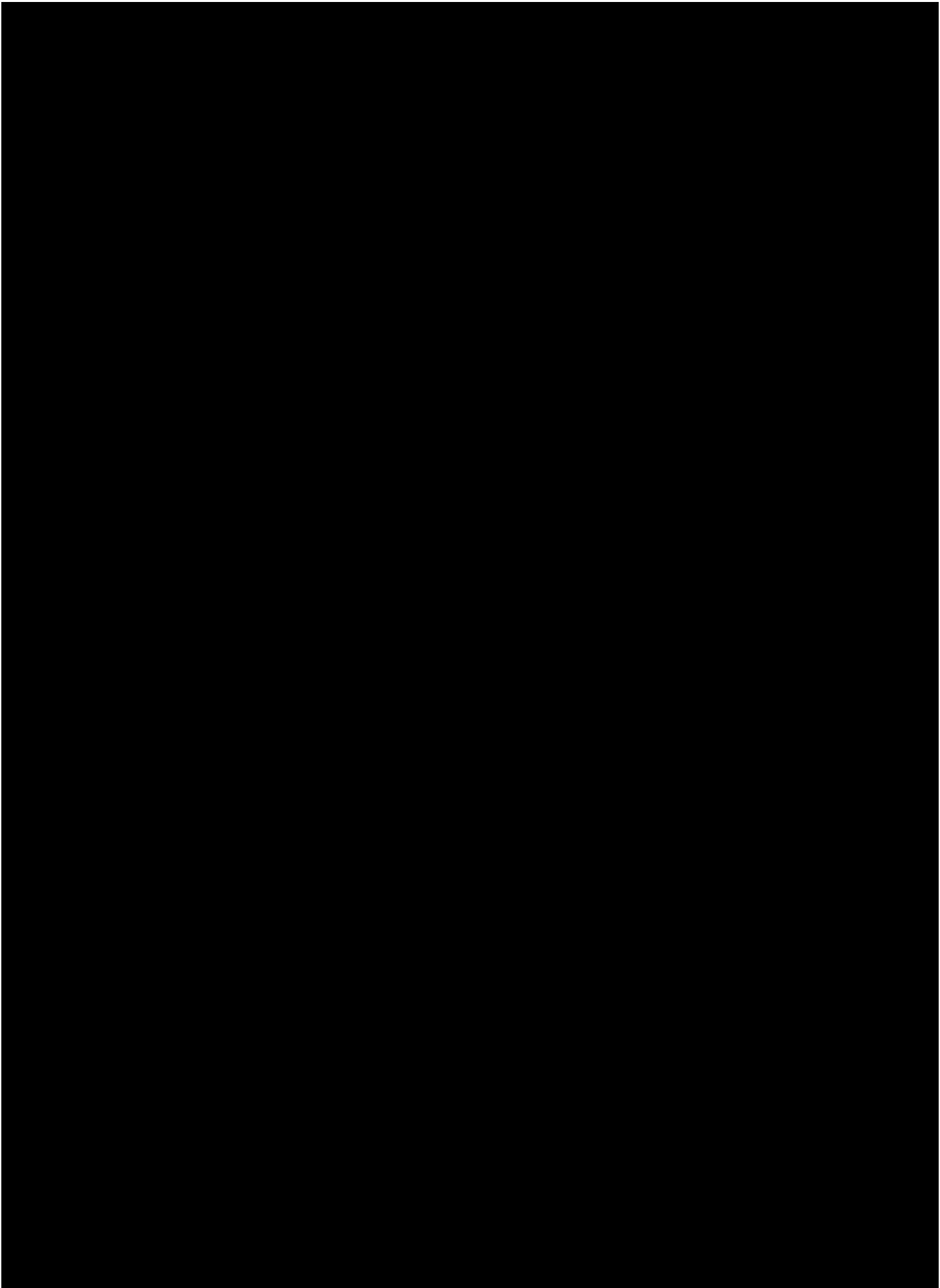
Annex 8 (Supplier TS Solution)

- 1 This Annex sets out the Supplier TS Solution and describes how the Transitional Services will be delivered during the TS Term.

ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

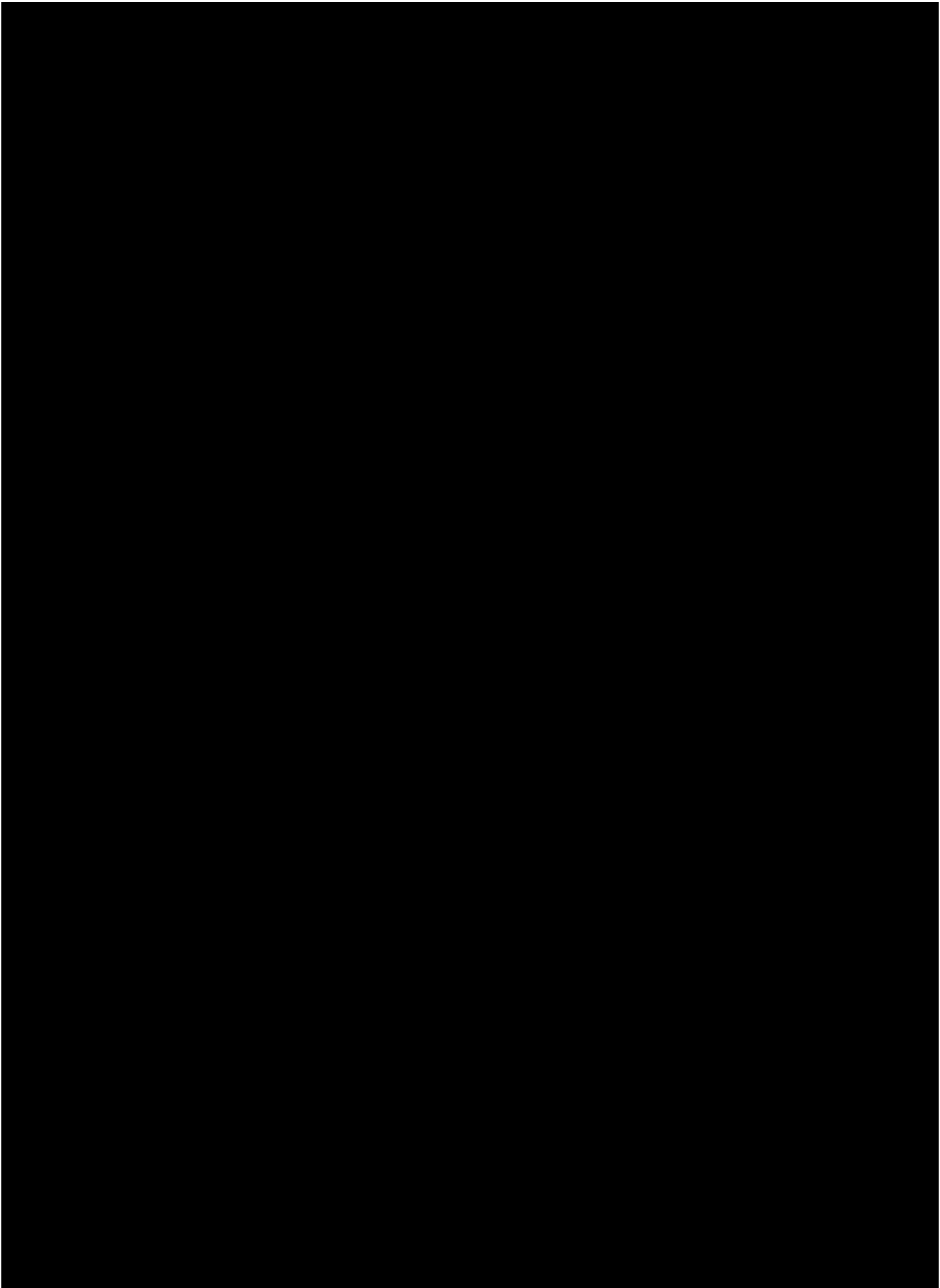
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

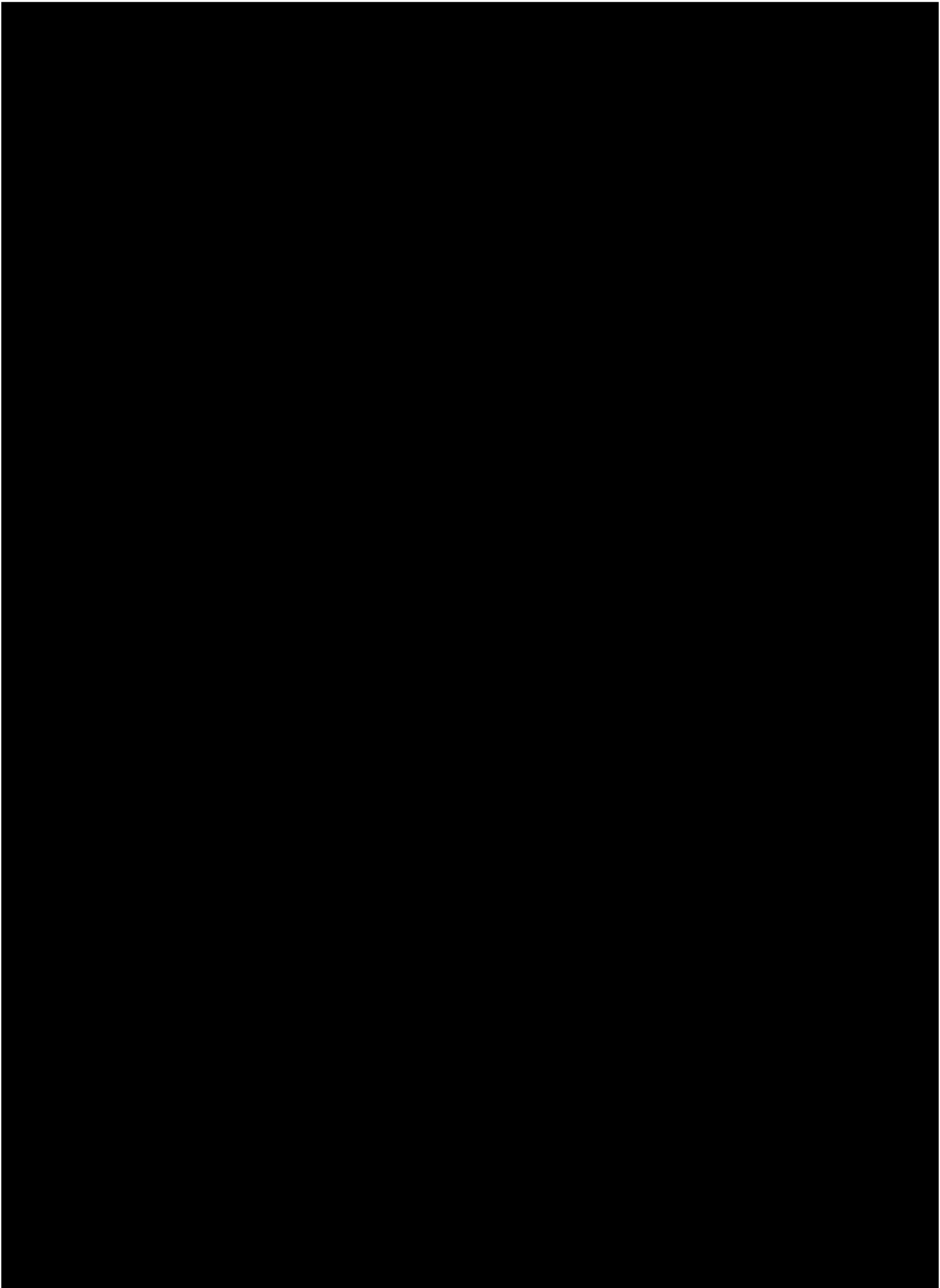
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

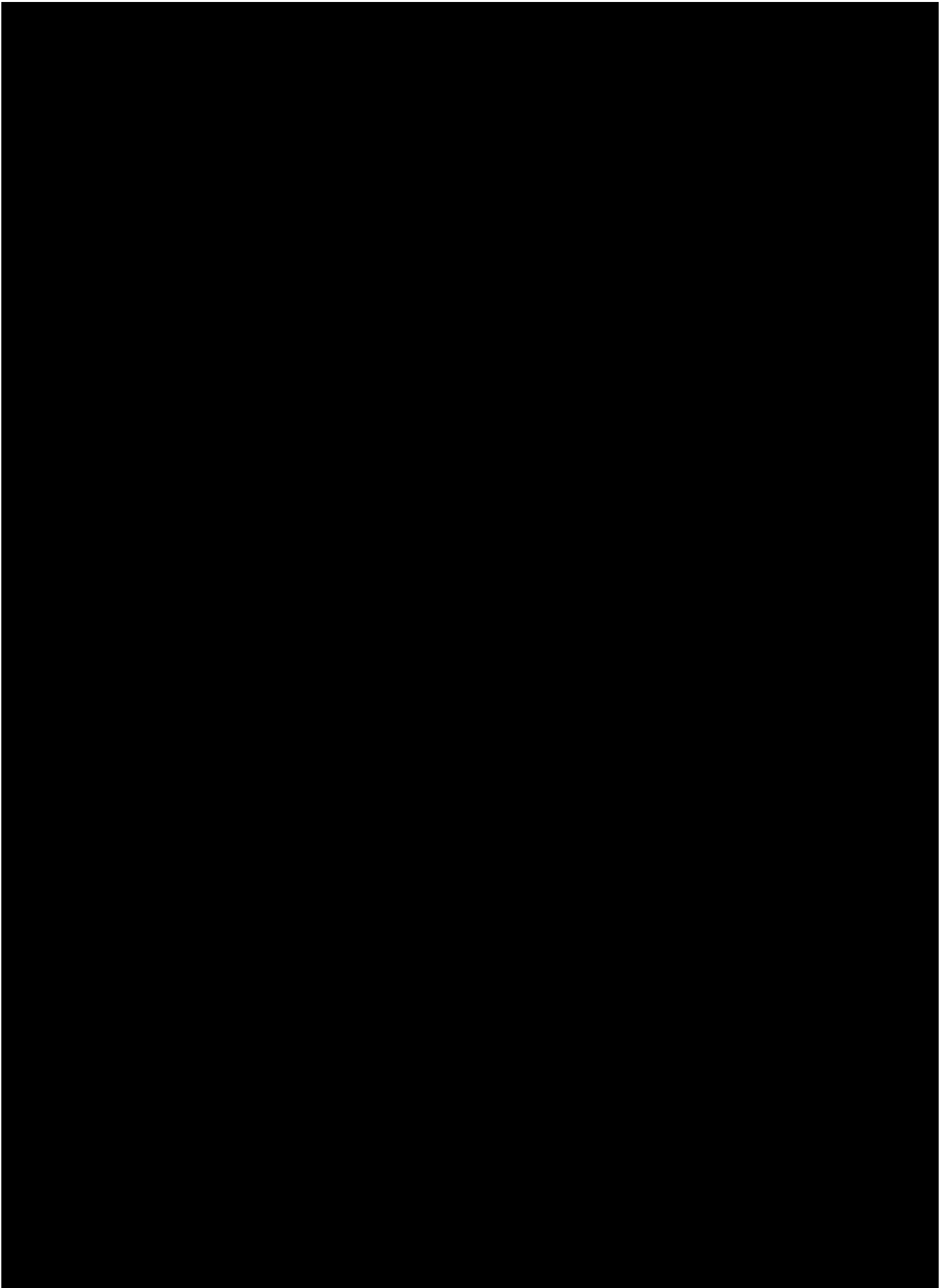
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

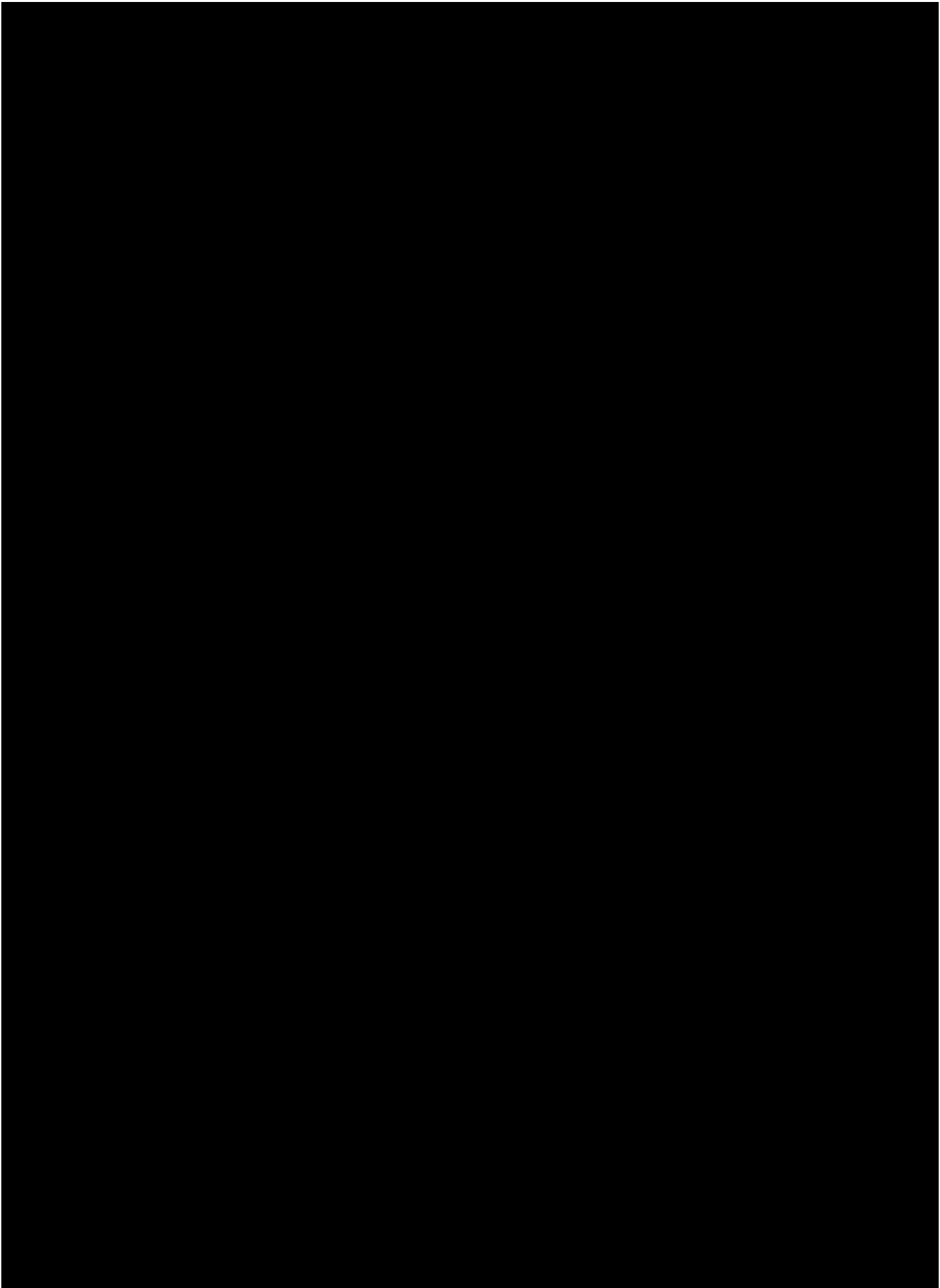
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



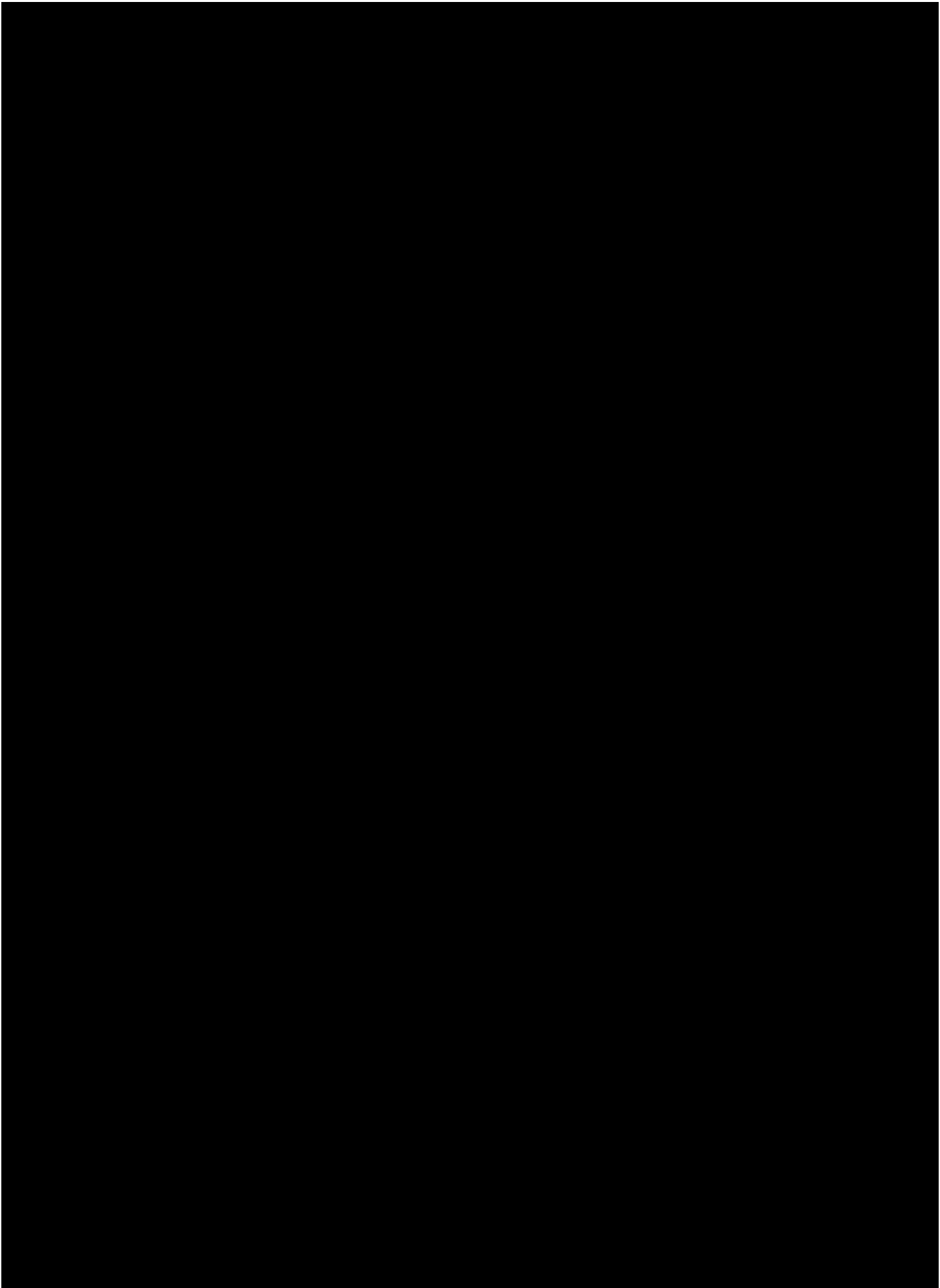
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]



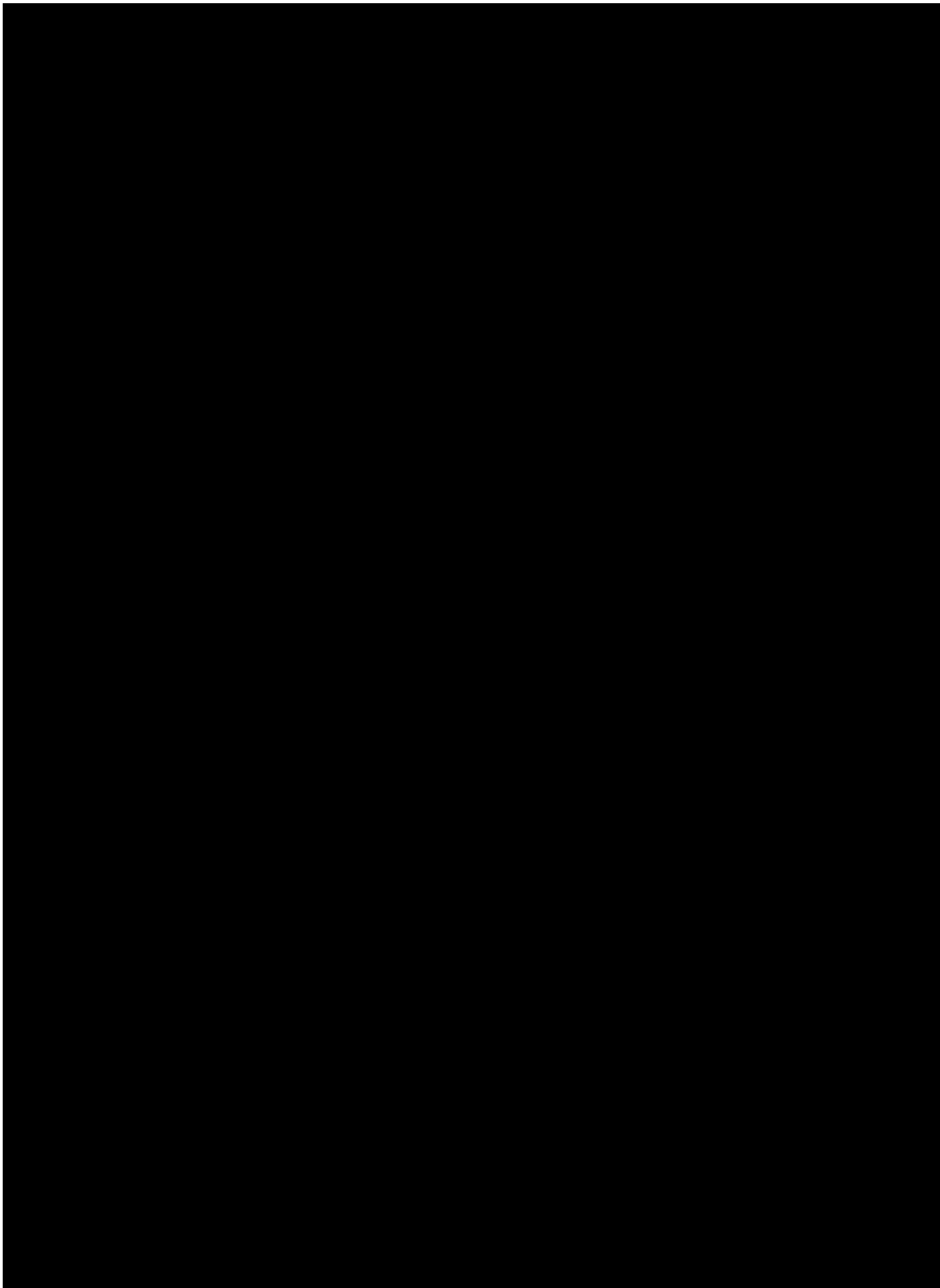
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

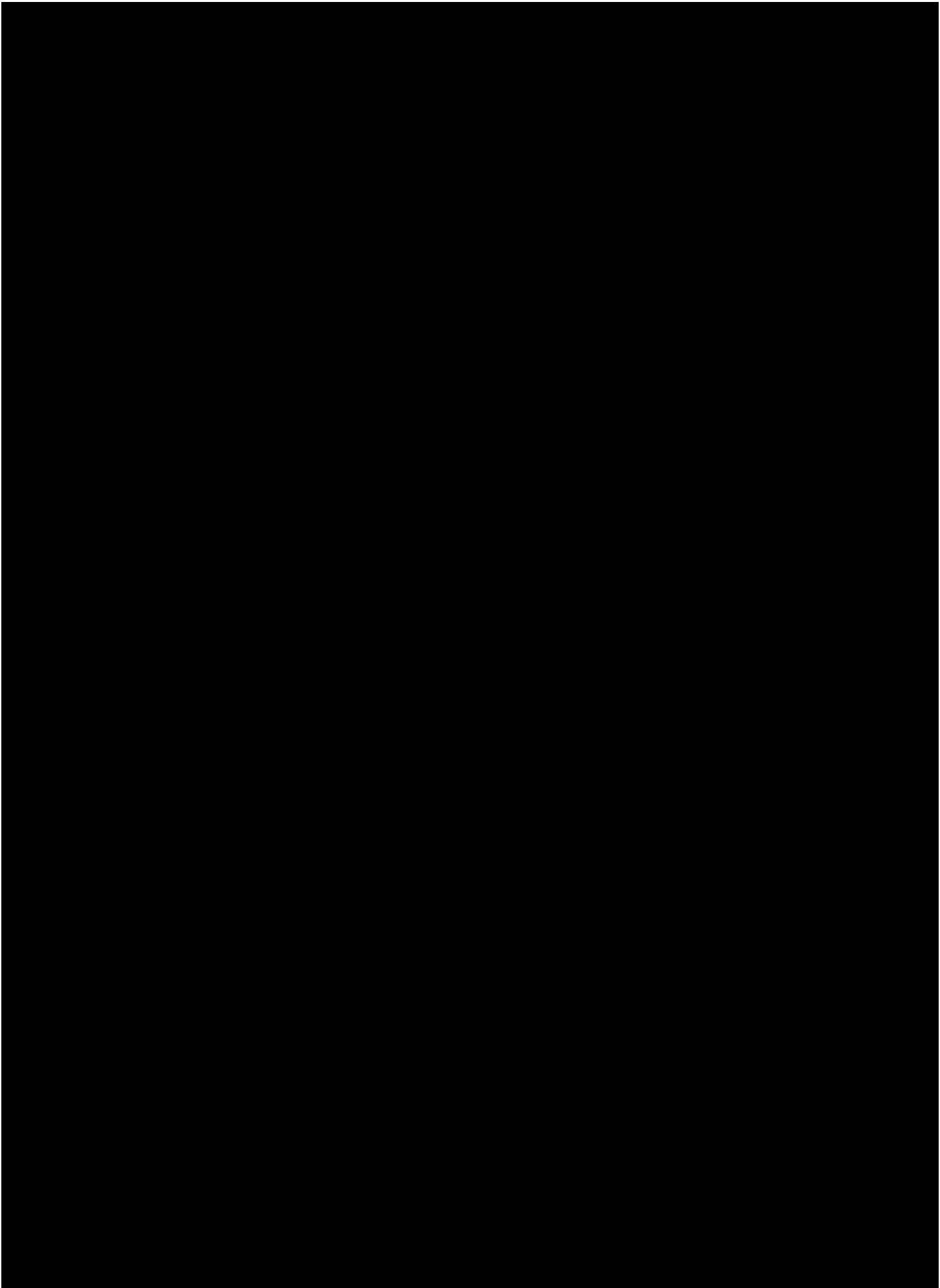
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



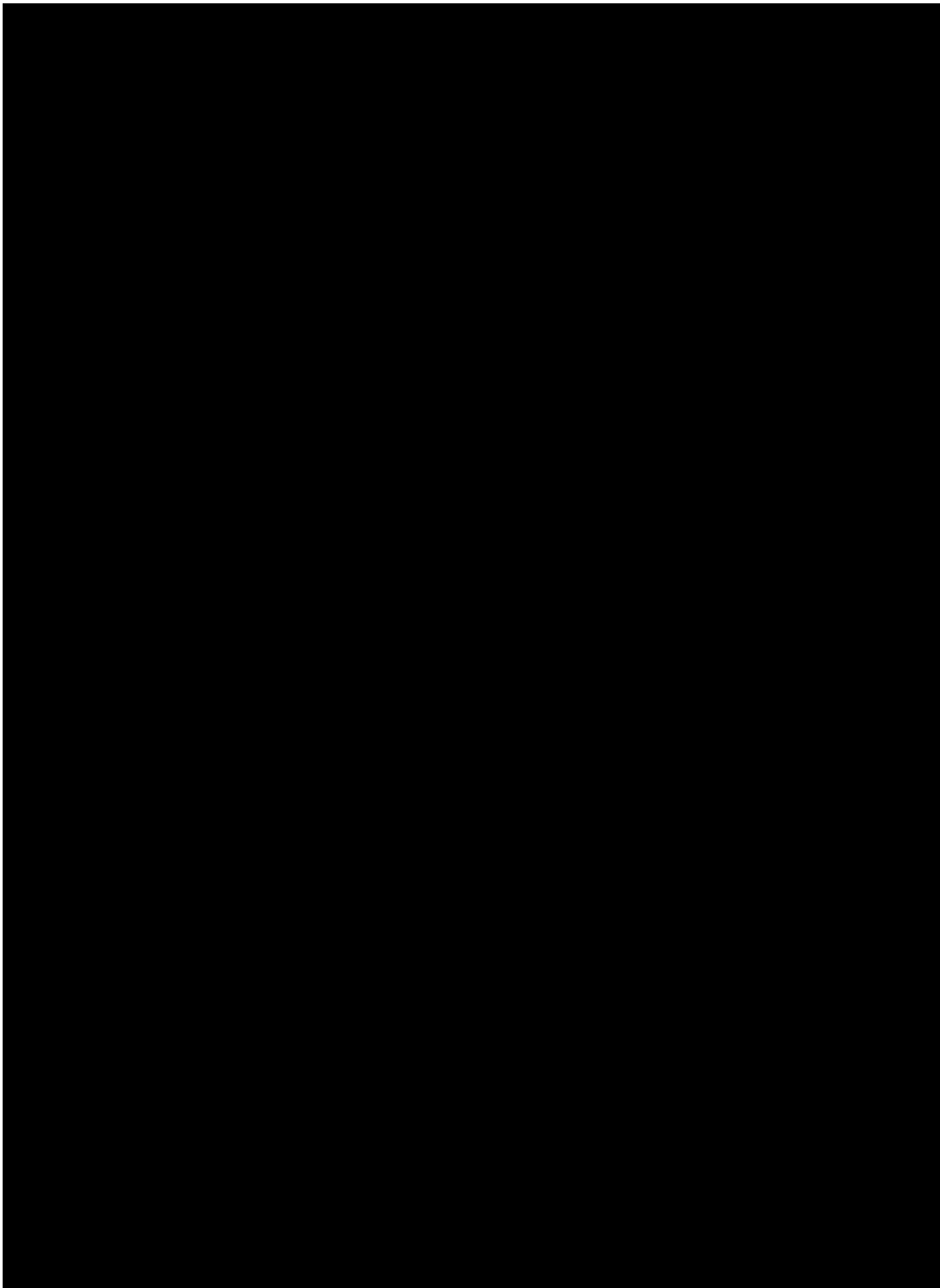
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

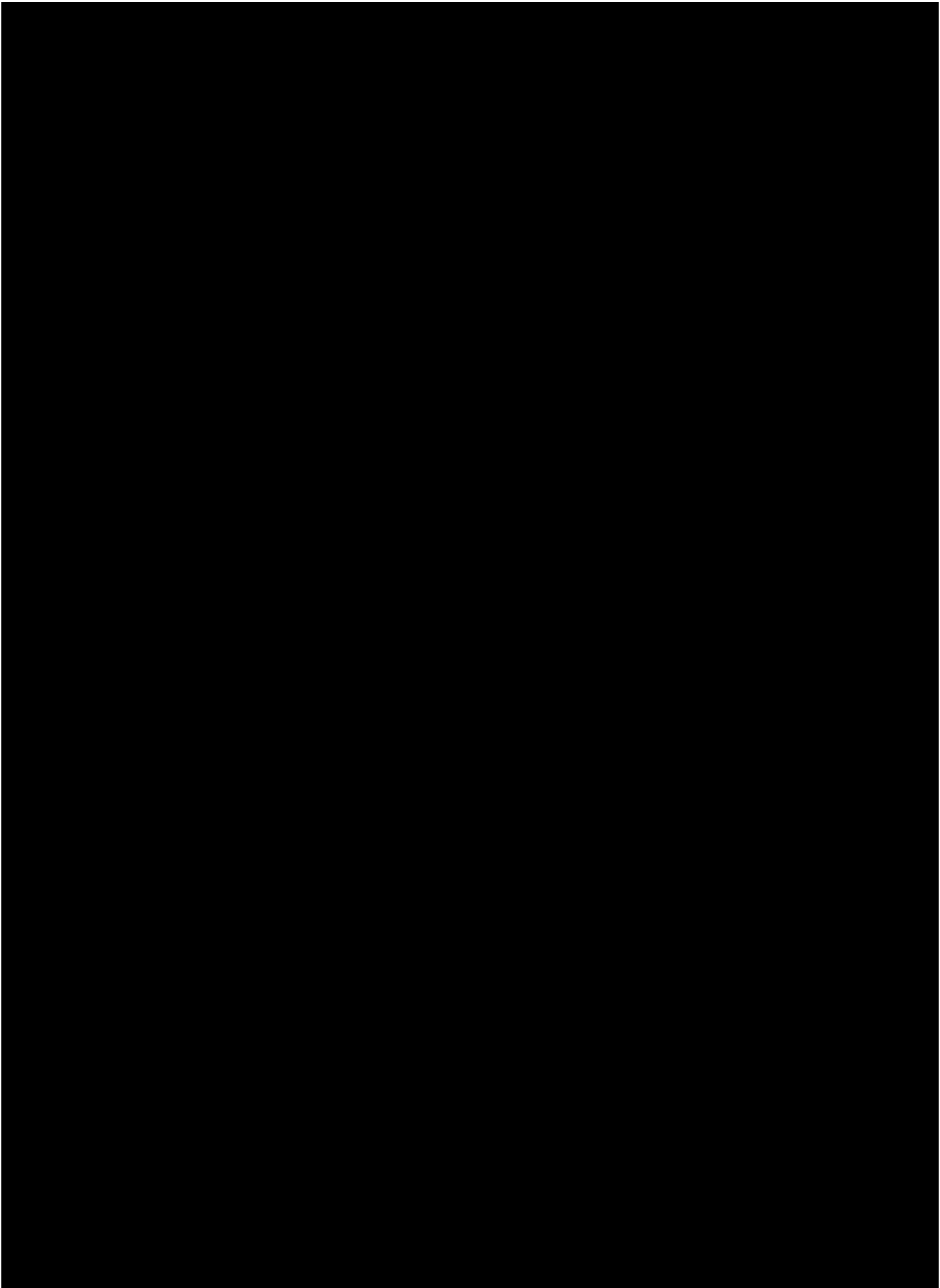
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

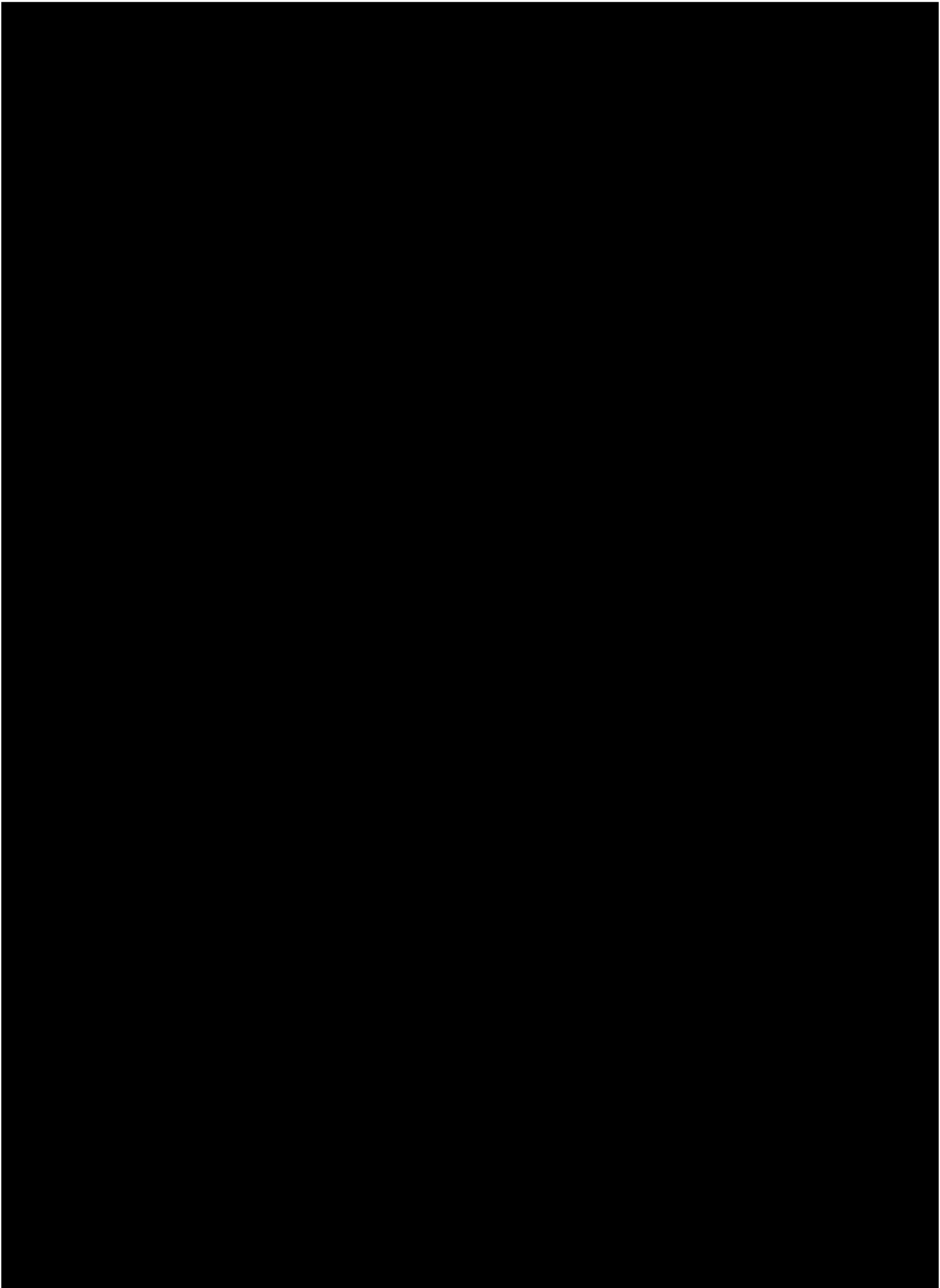
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

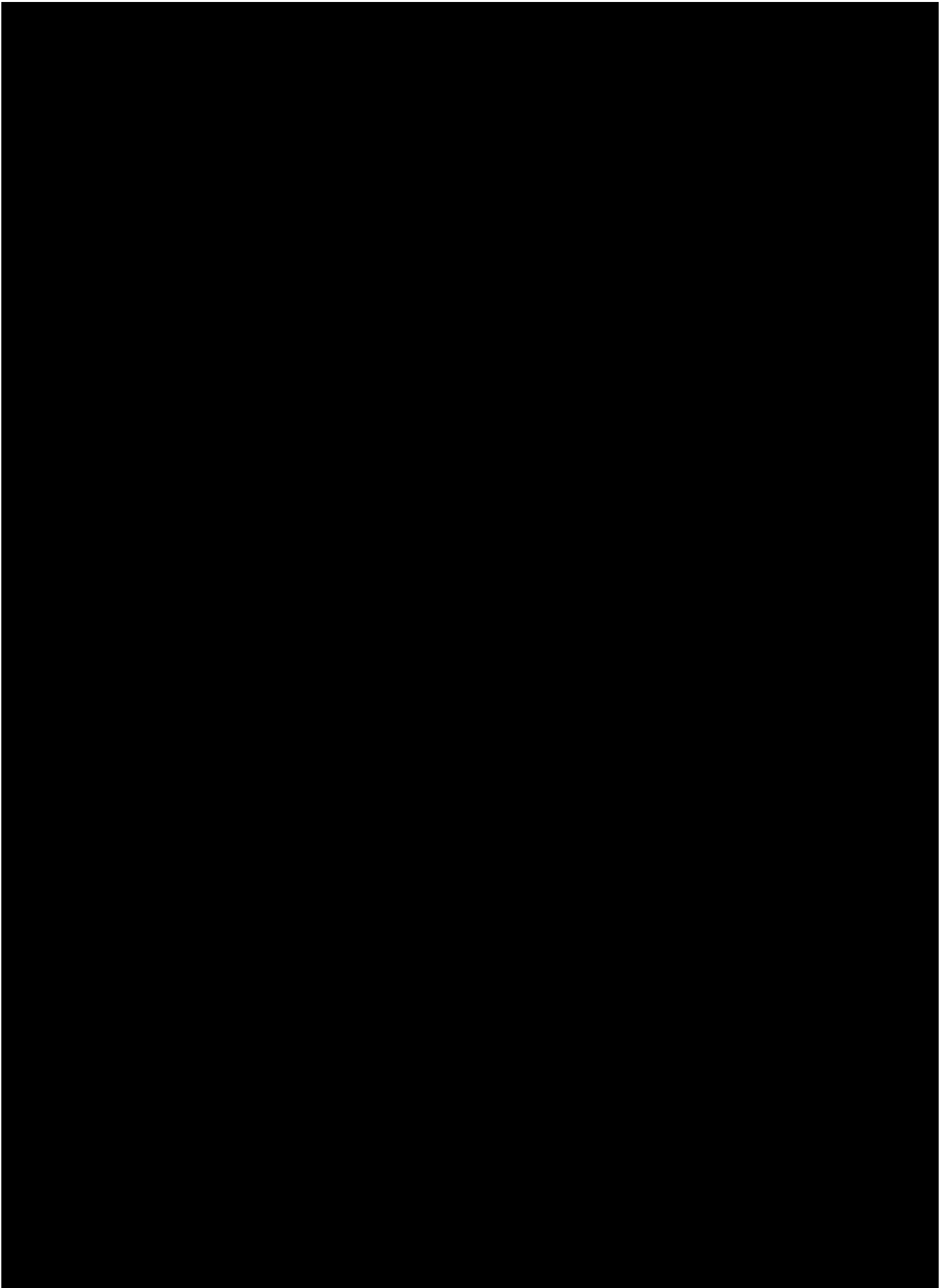
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

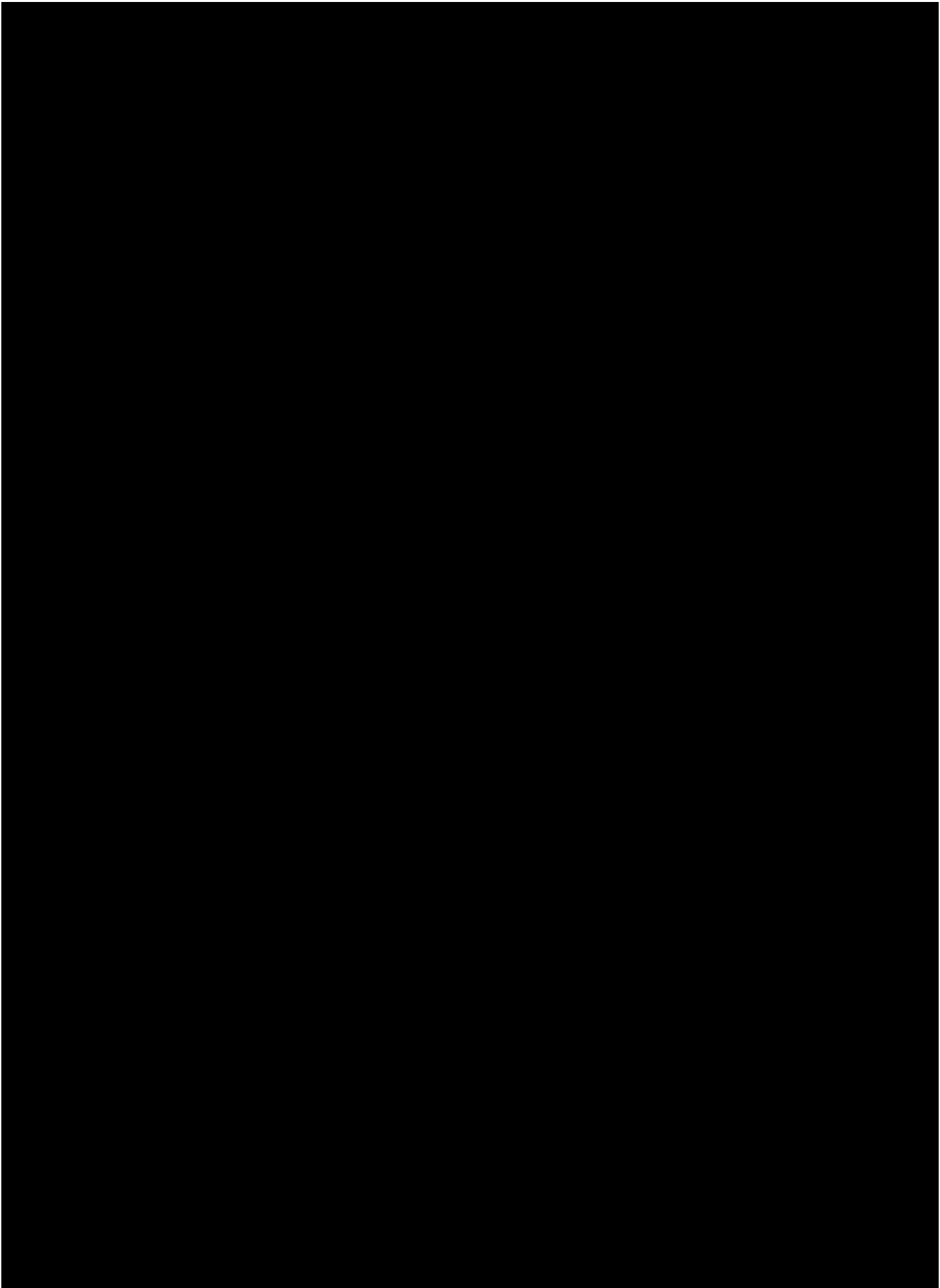
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

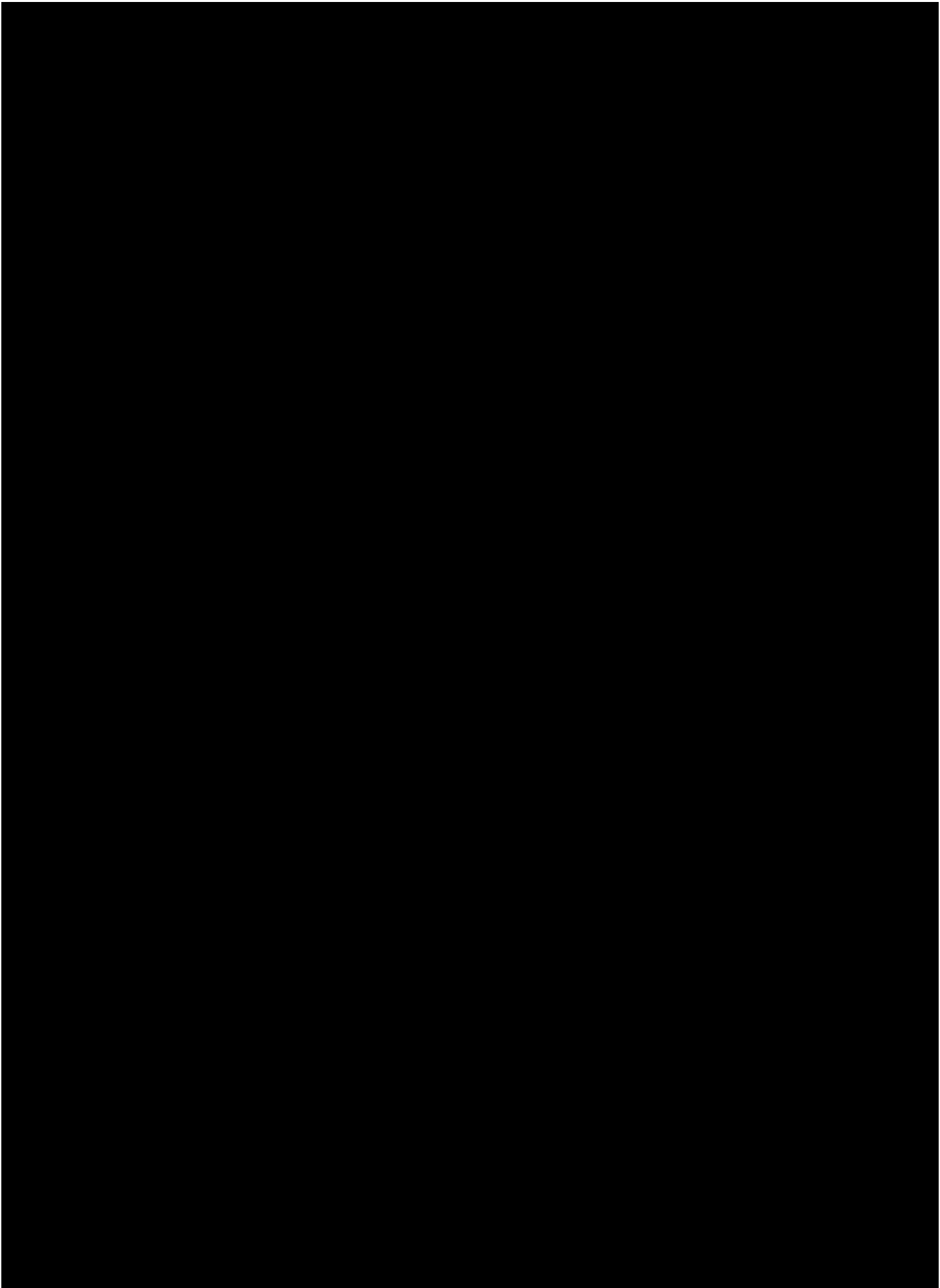
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

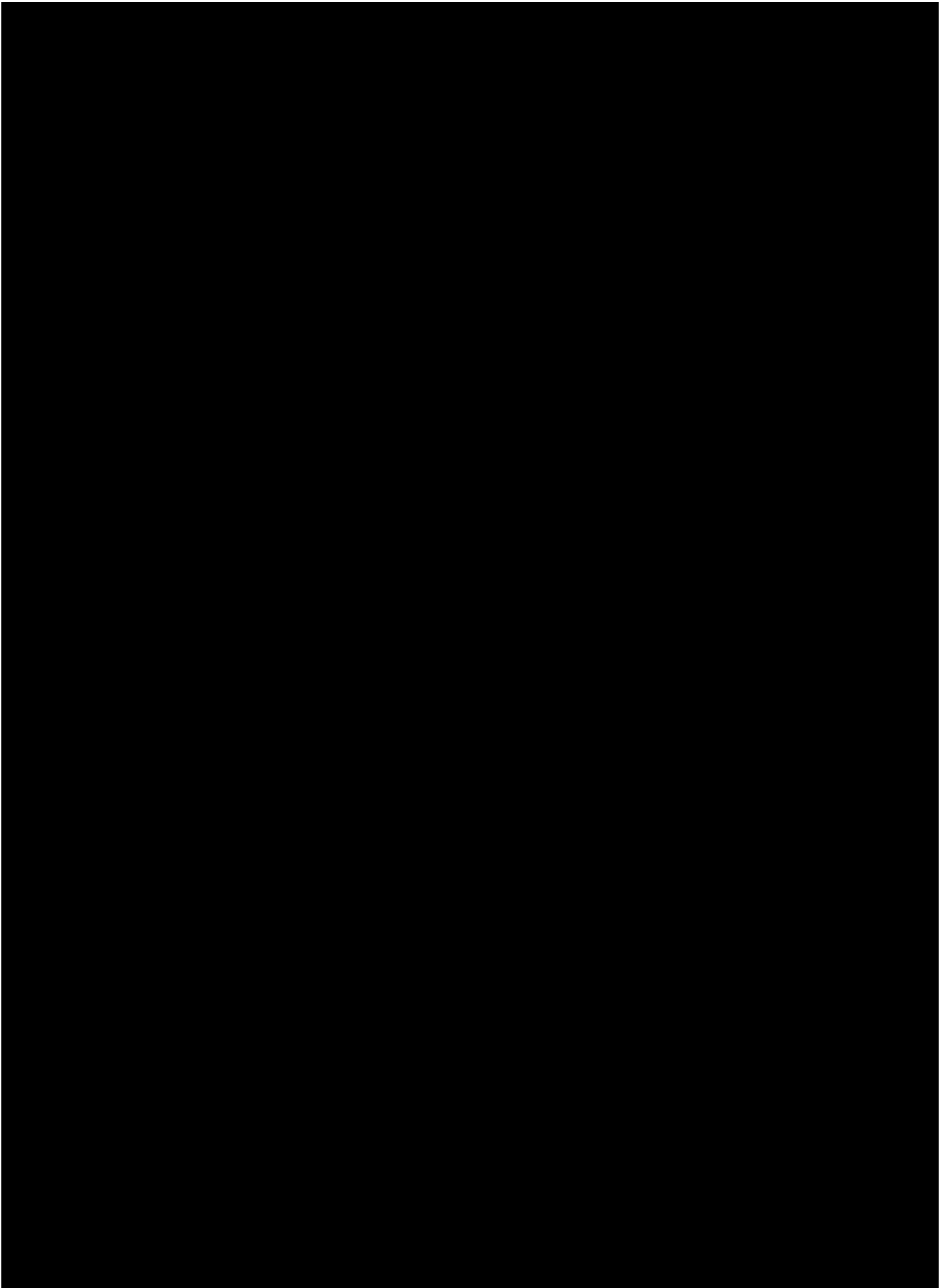
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

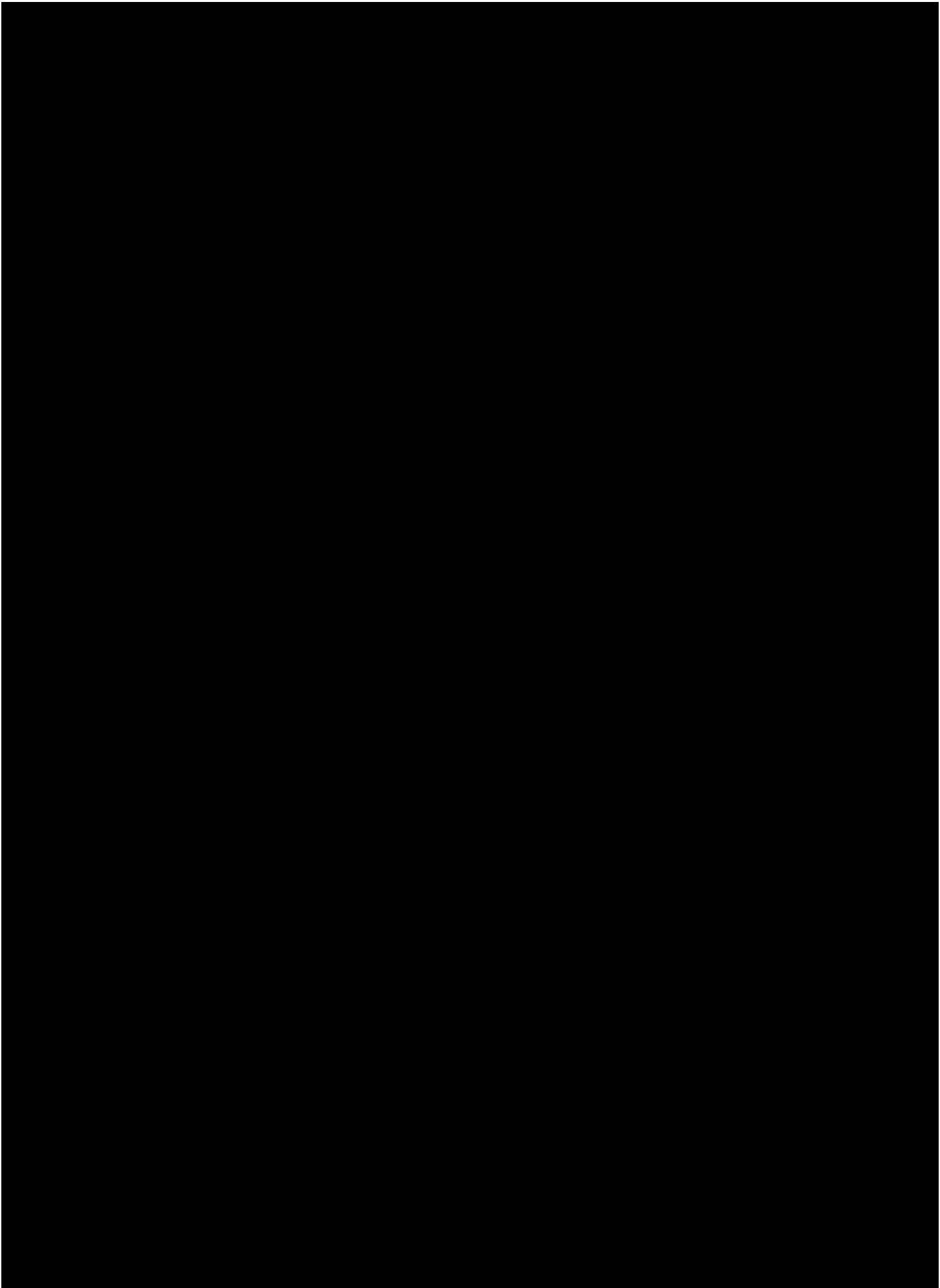
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



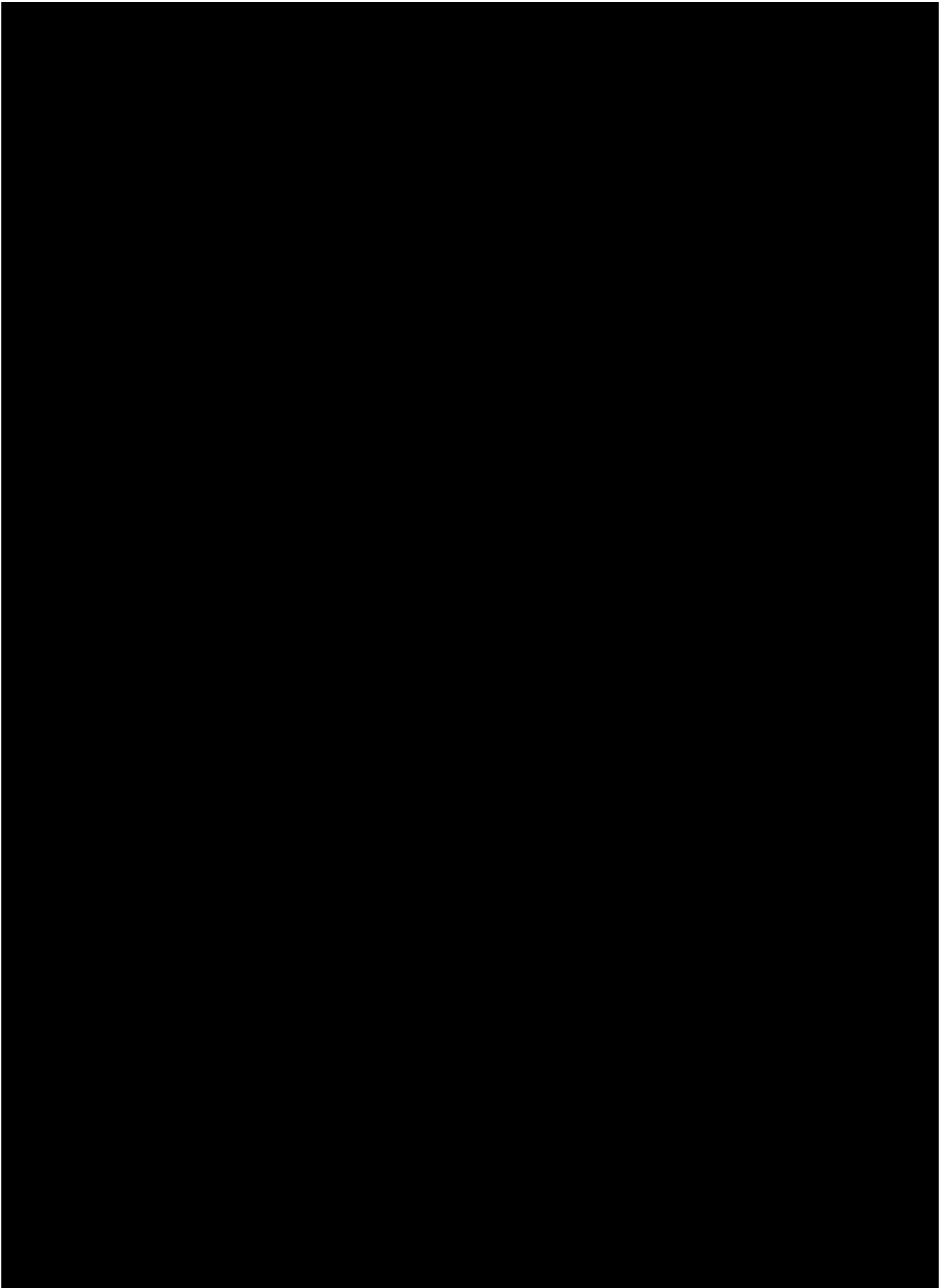
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

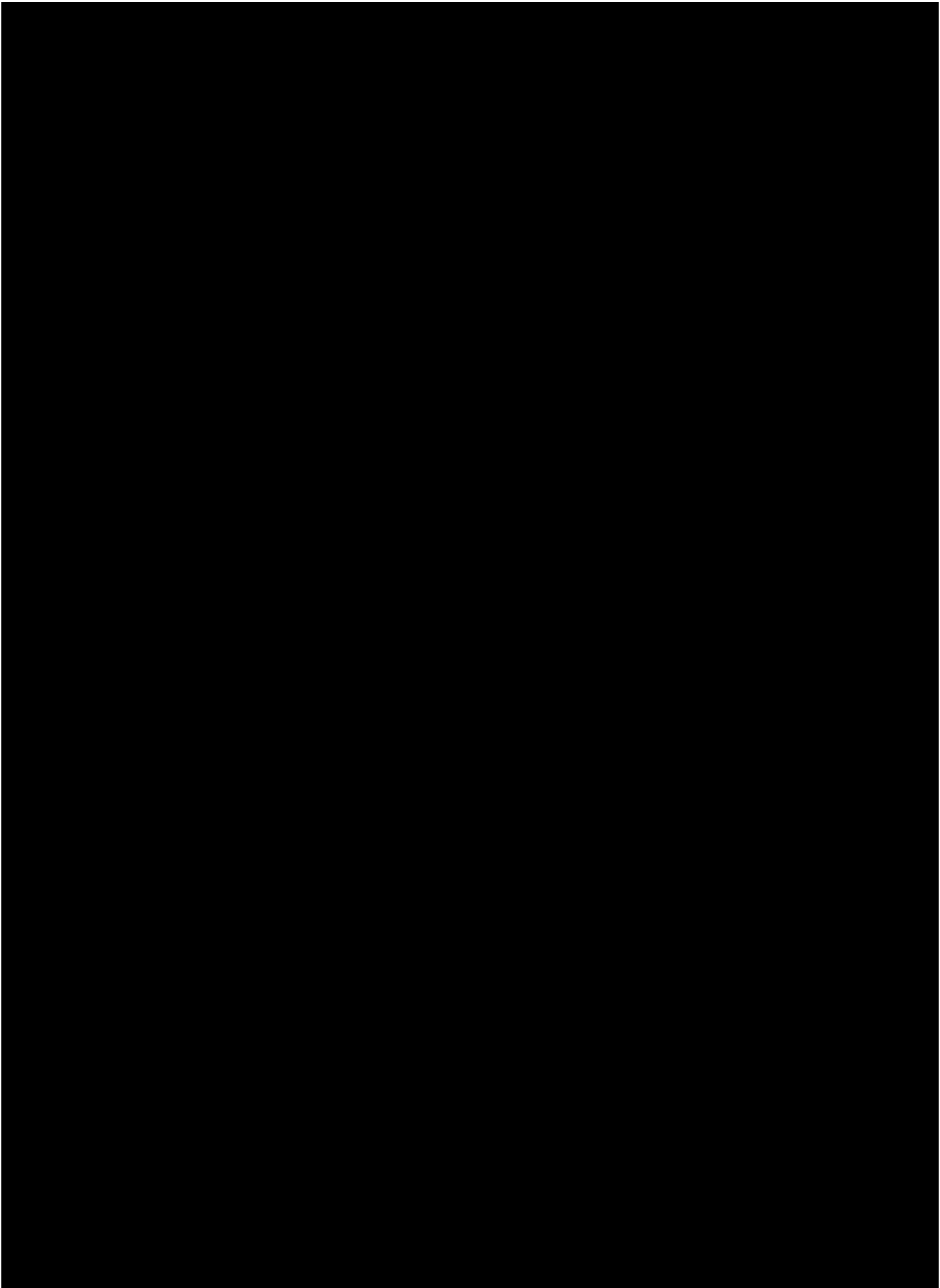
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



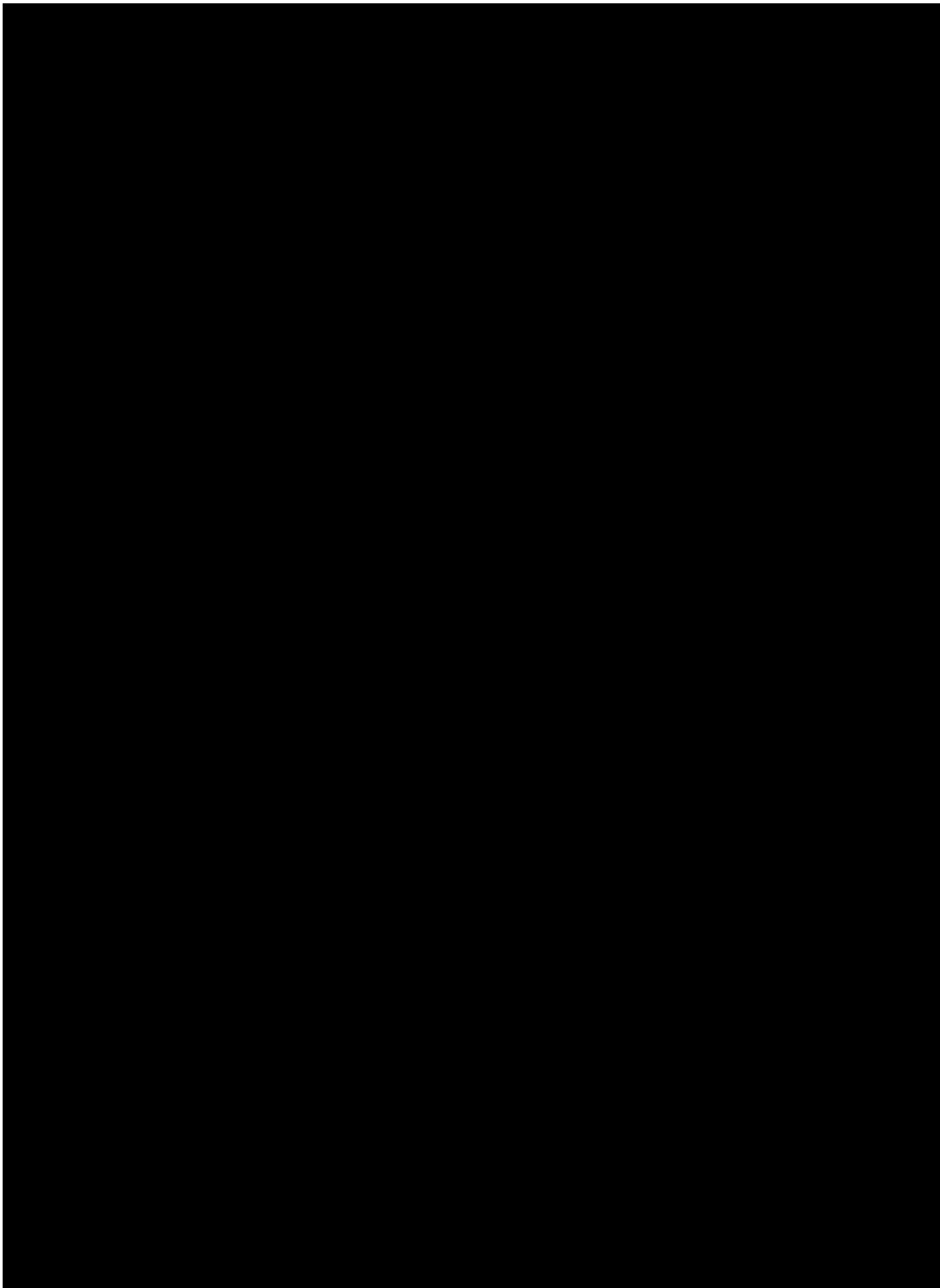
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]



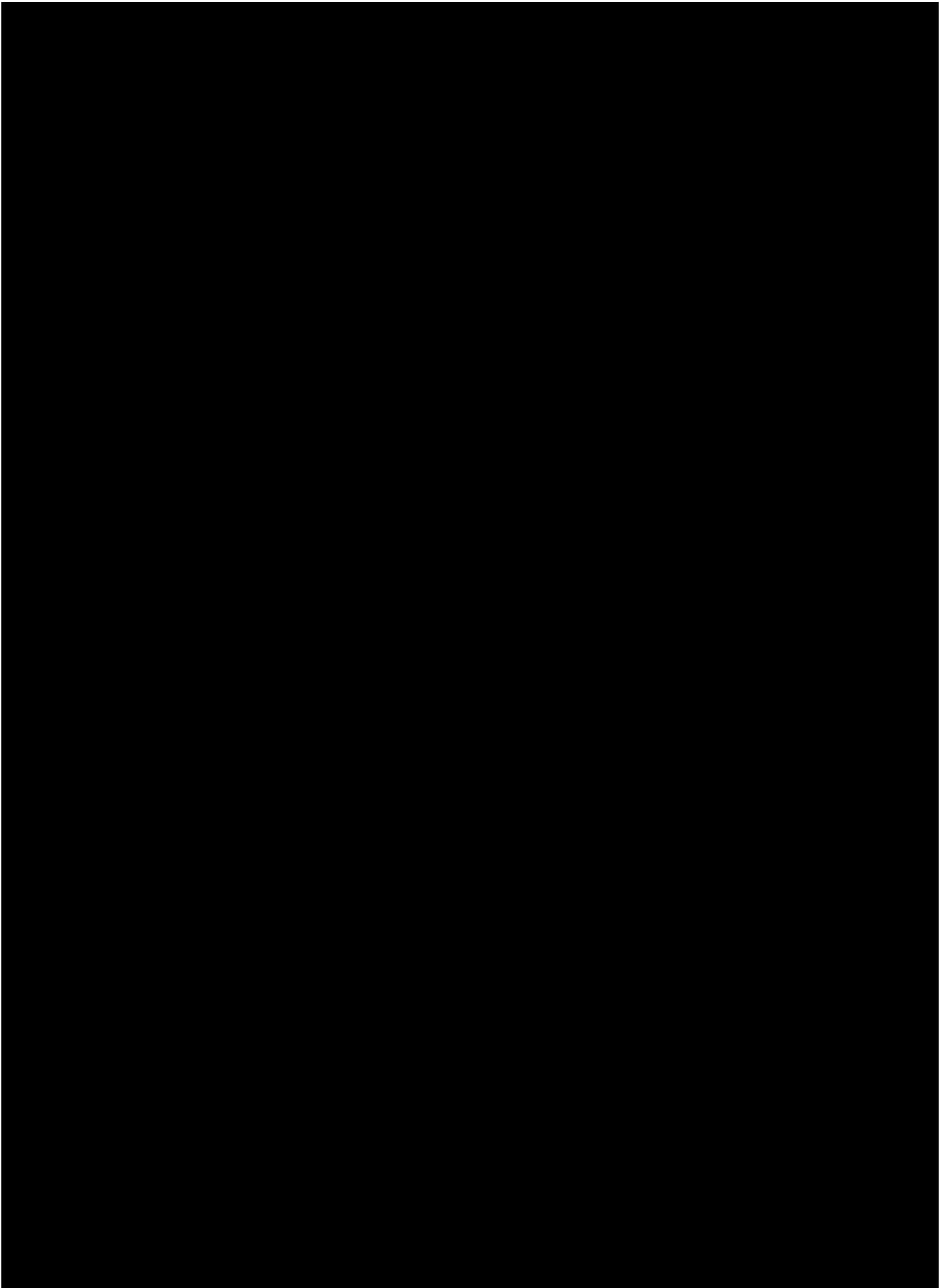
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

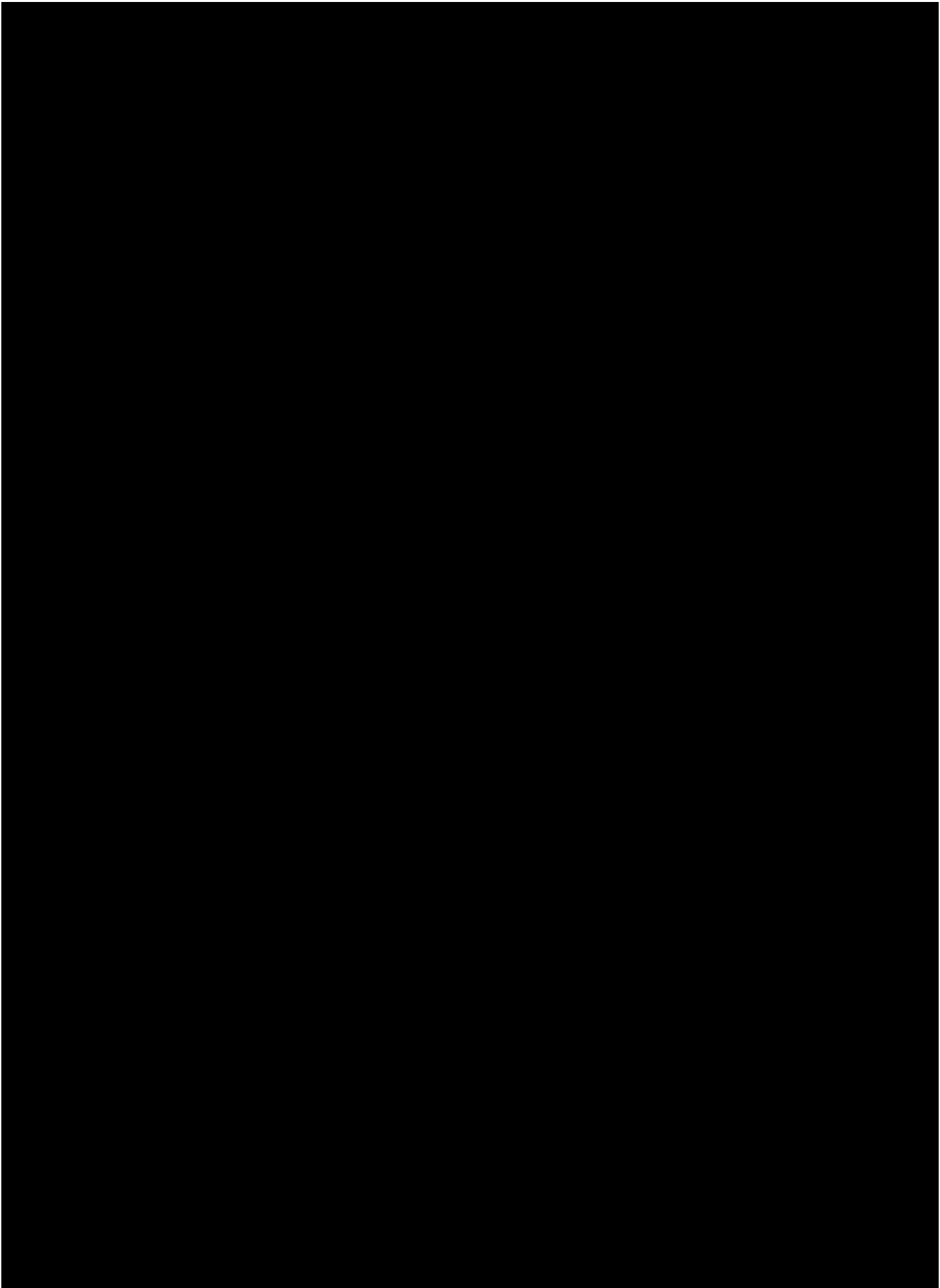
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



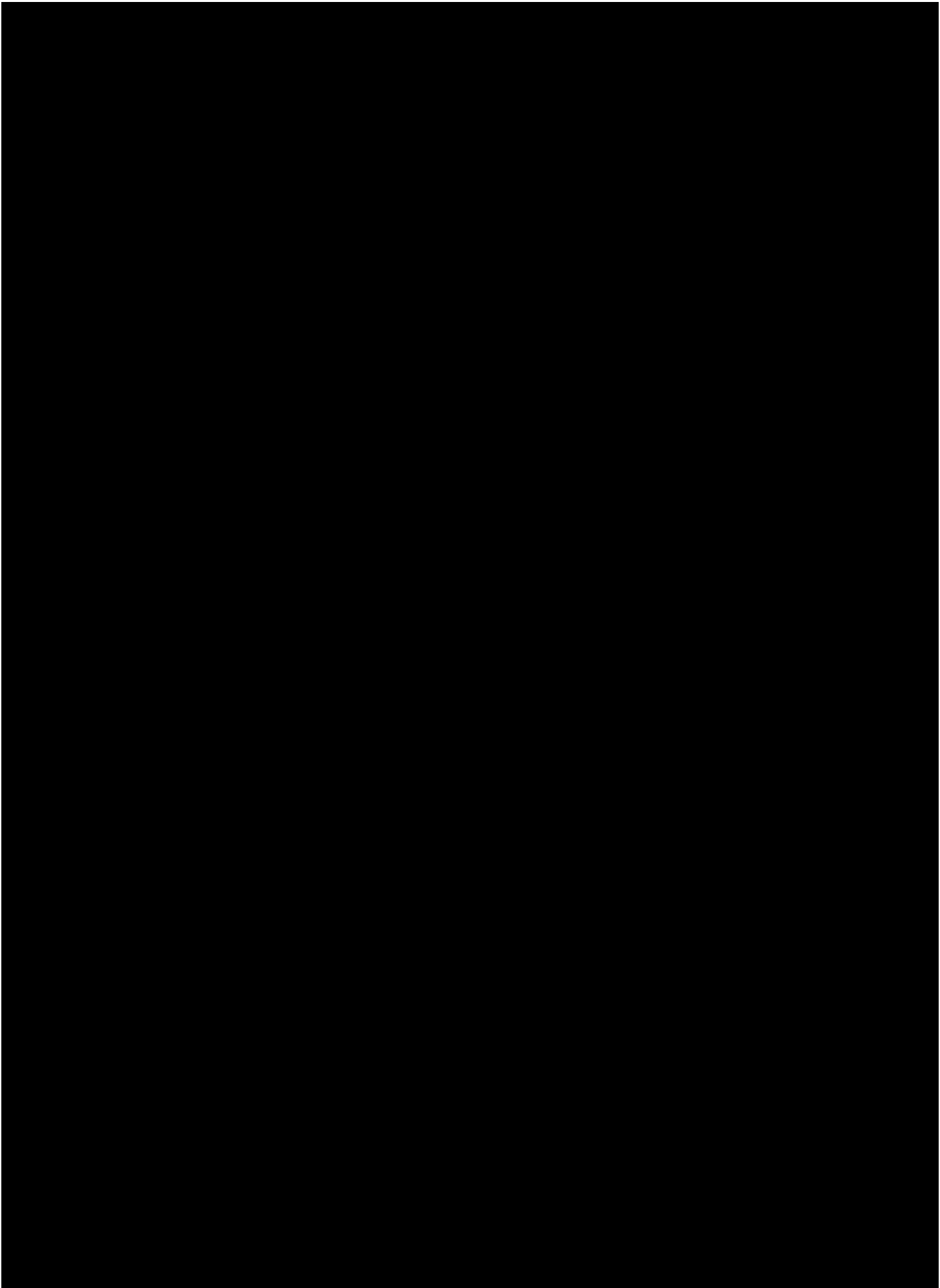
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

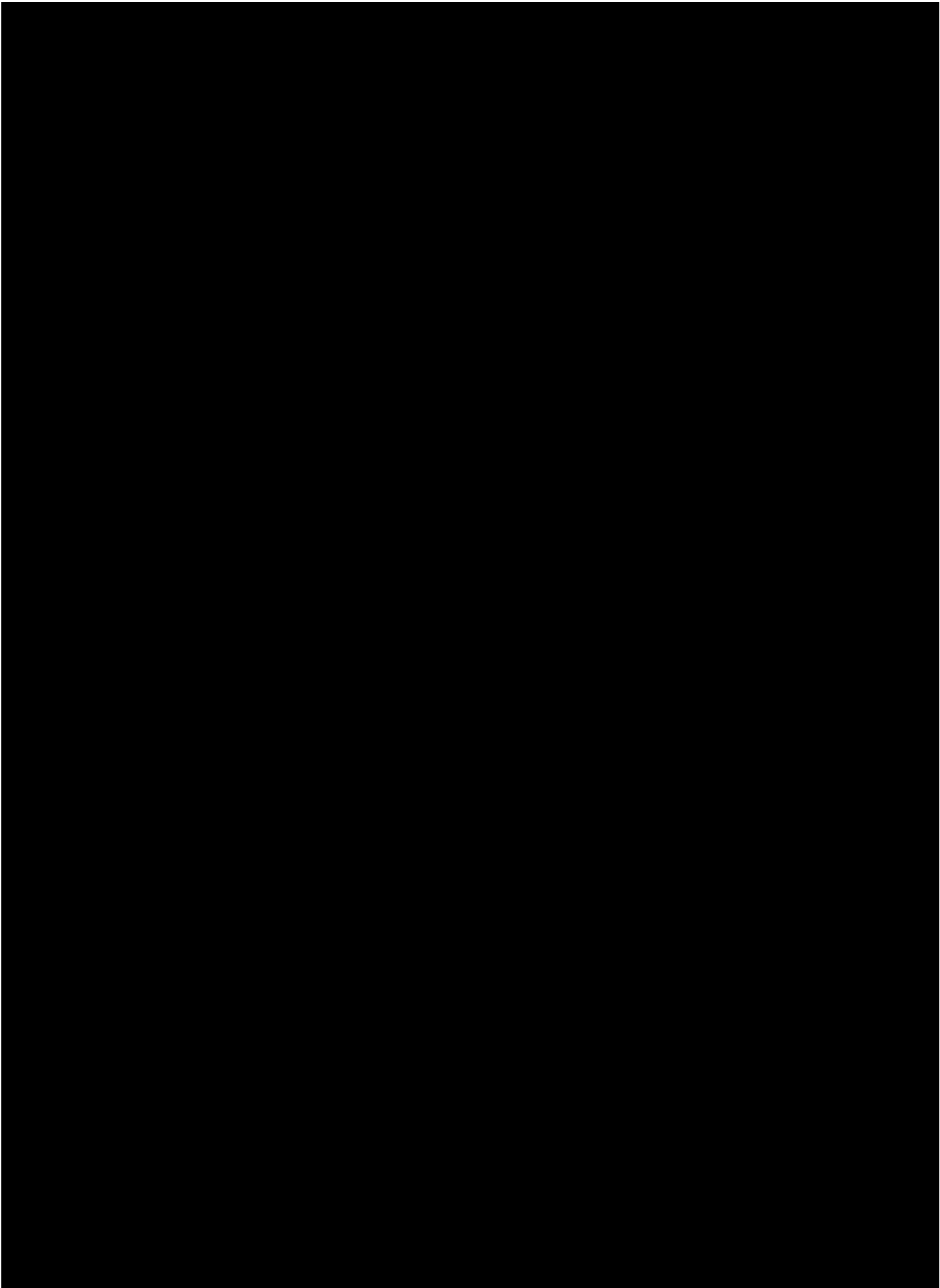
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

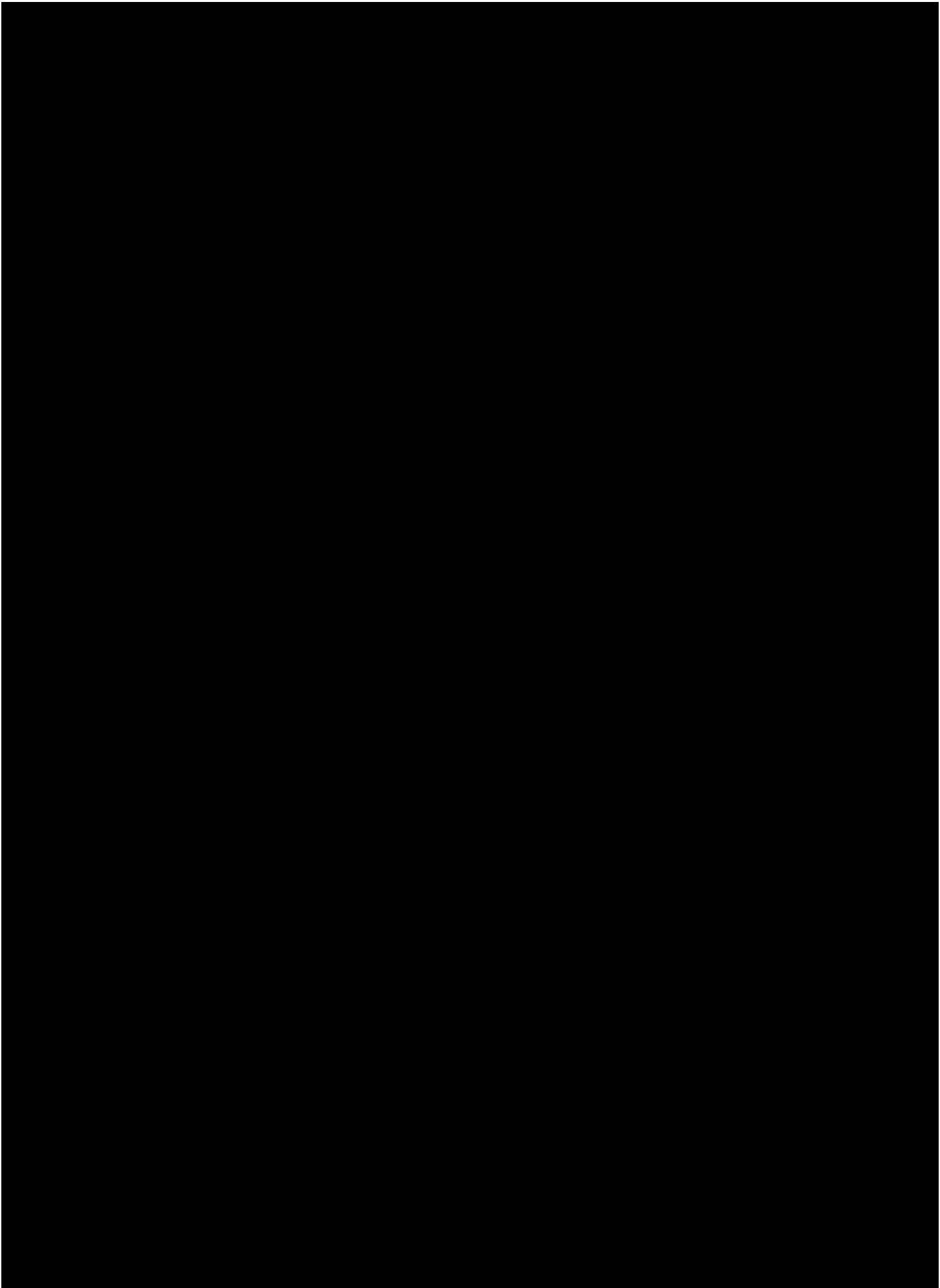
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

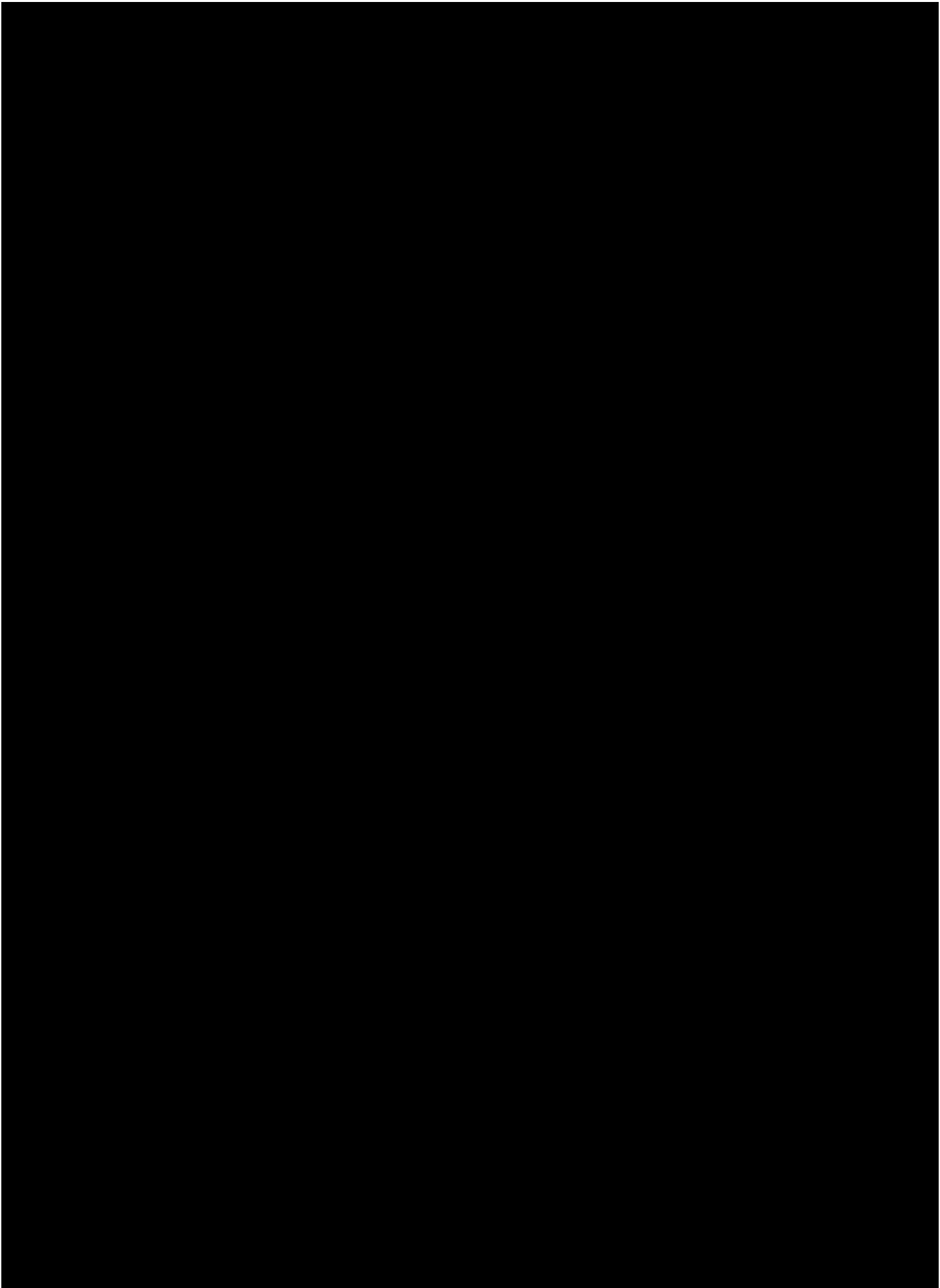
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



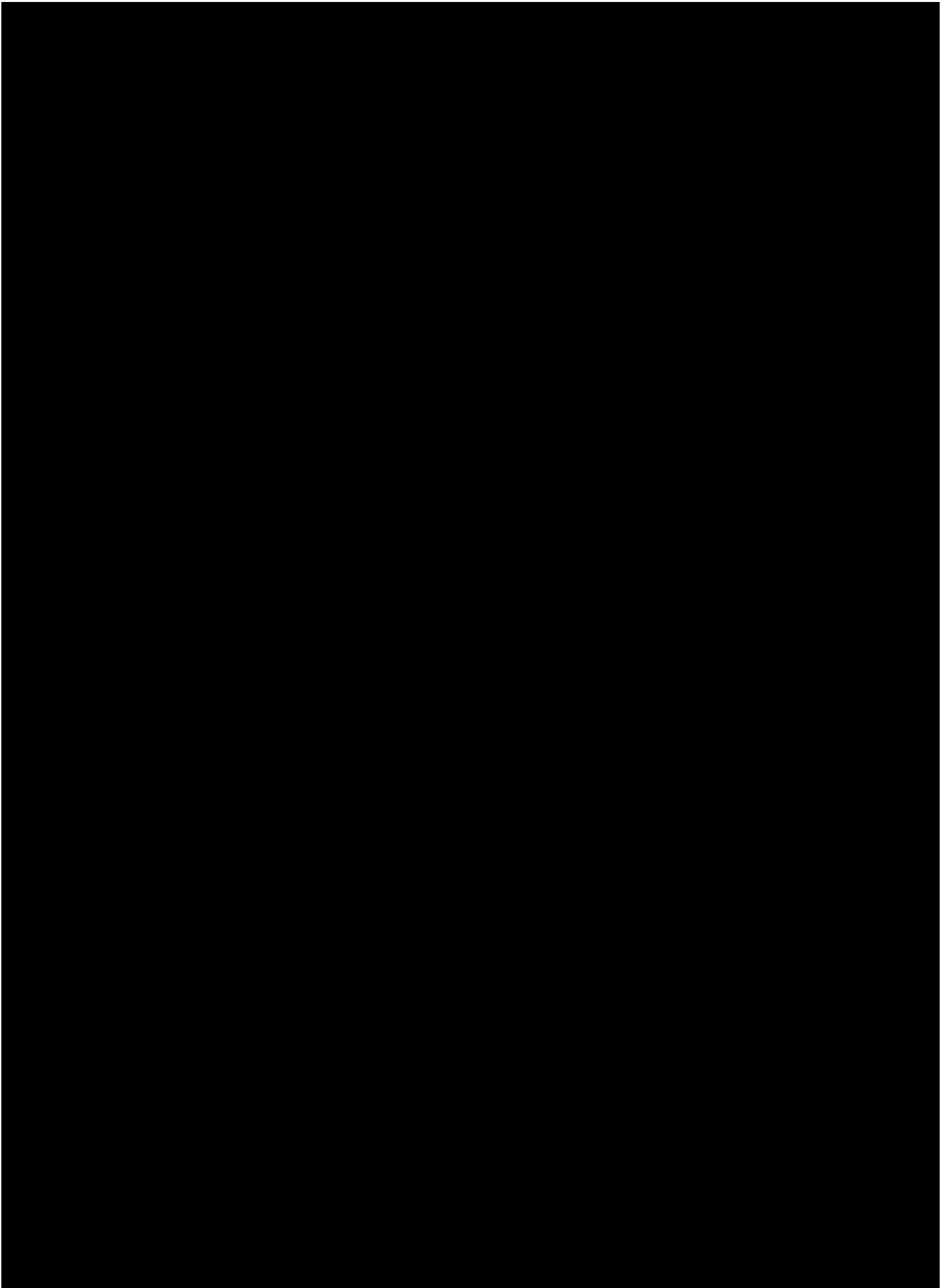
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

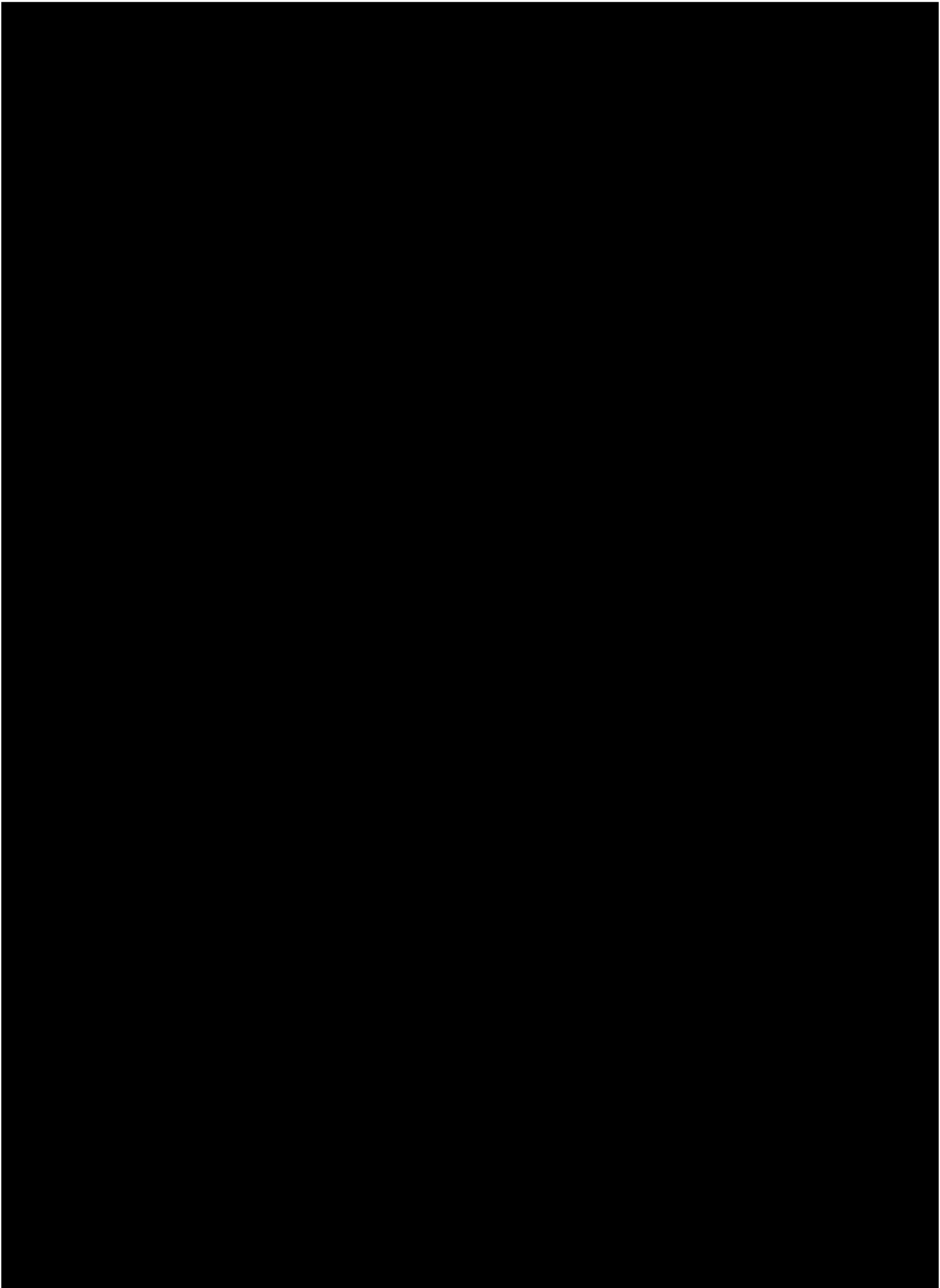
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

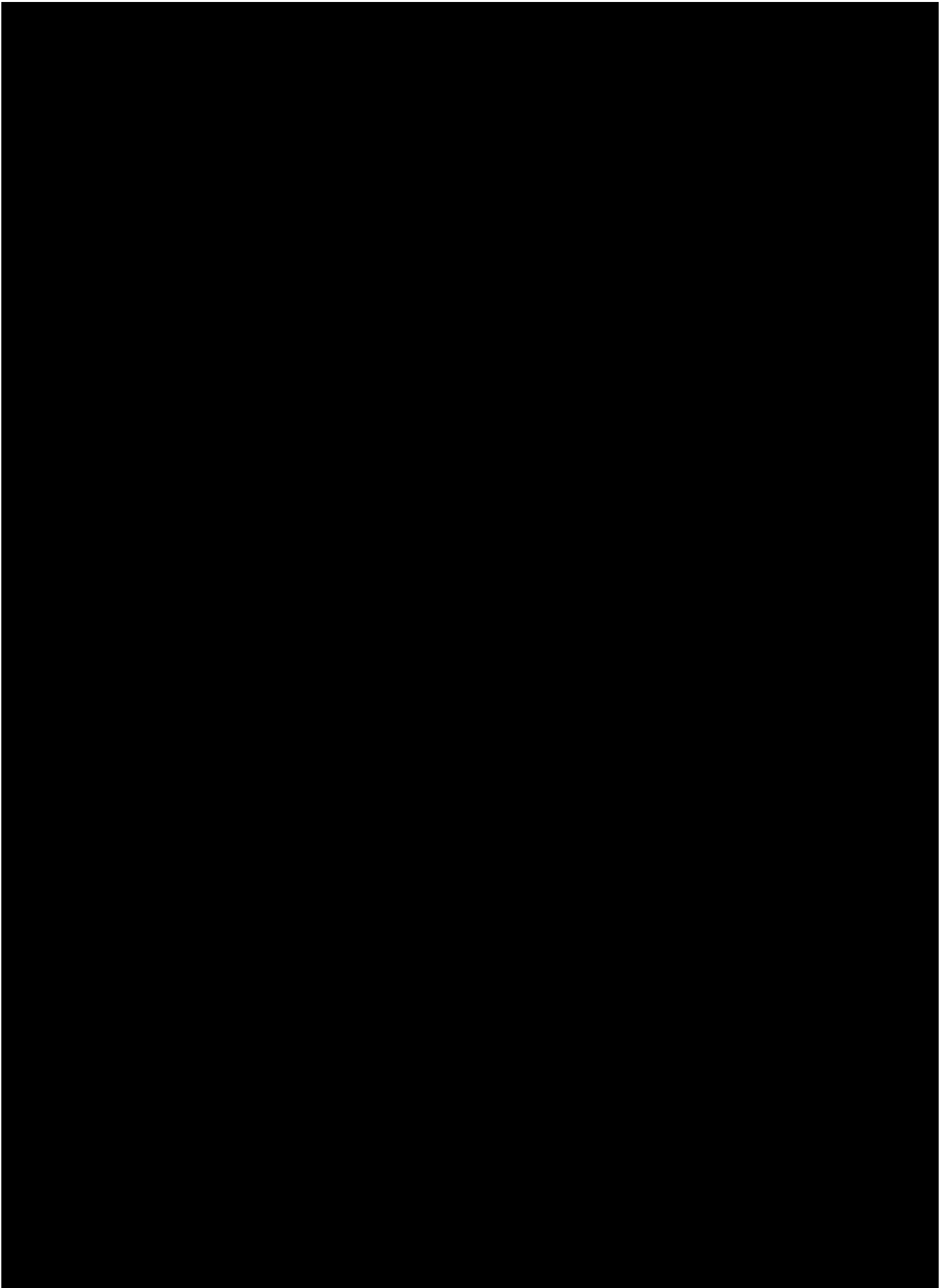
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

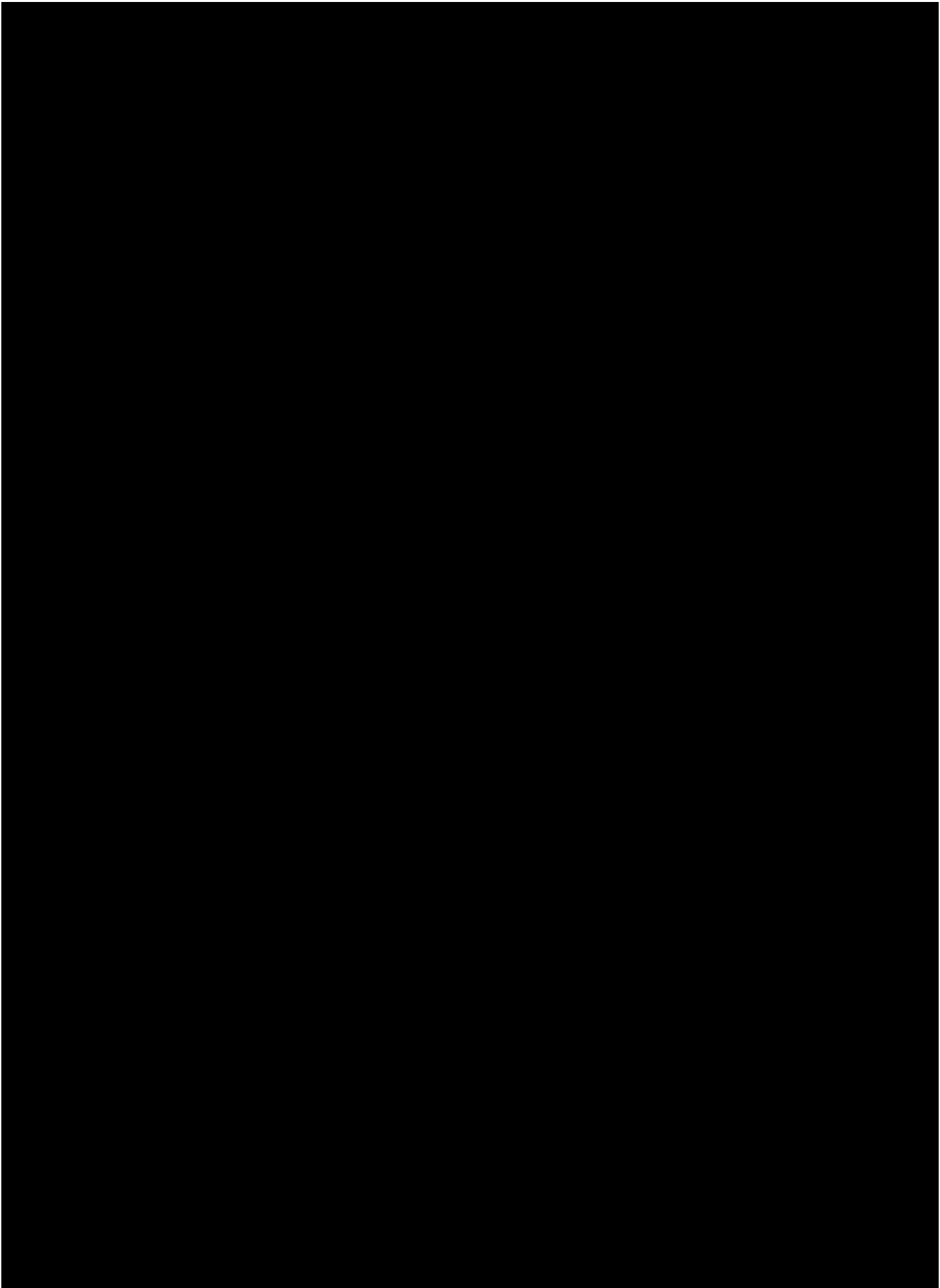
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



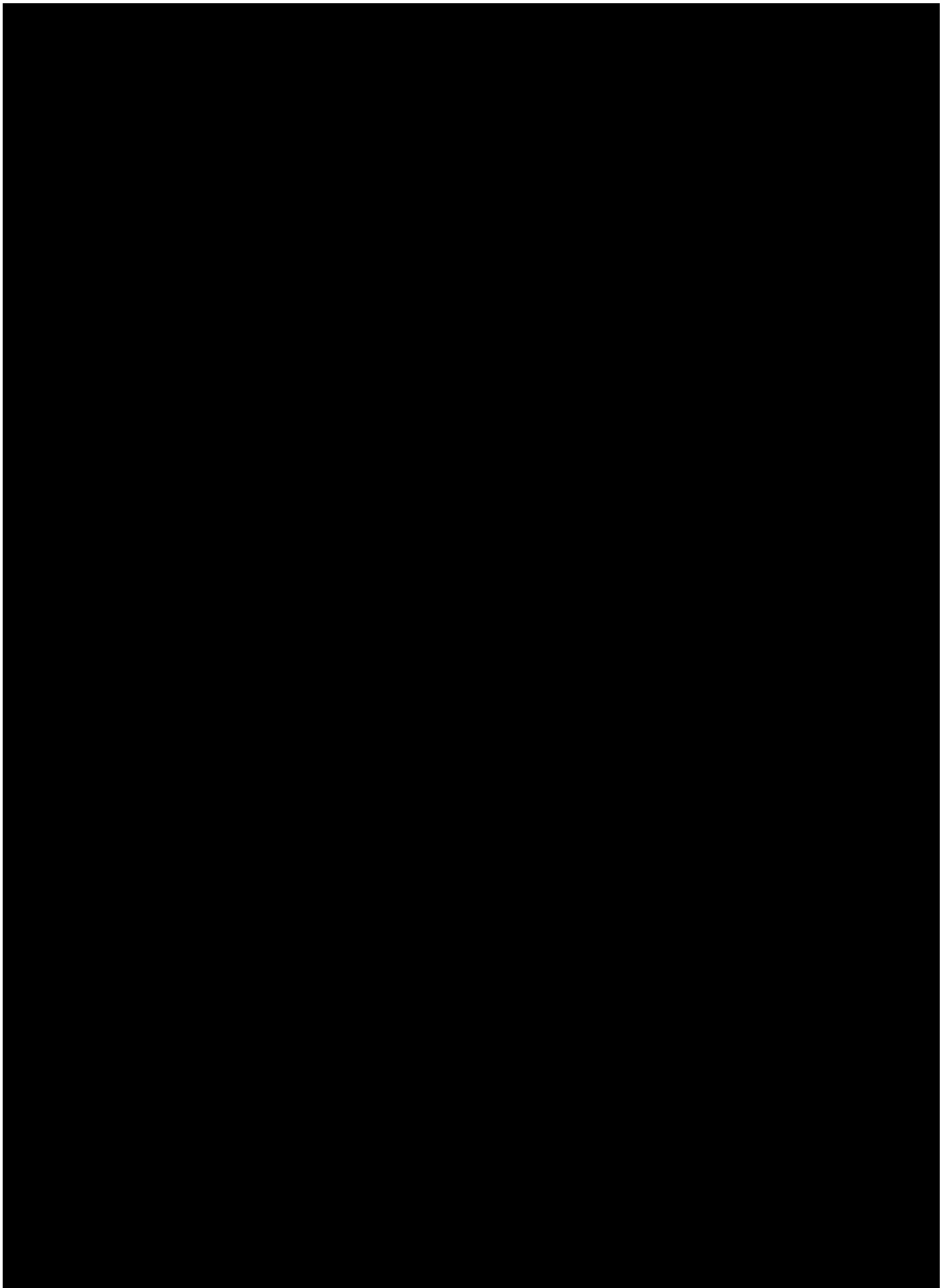
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

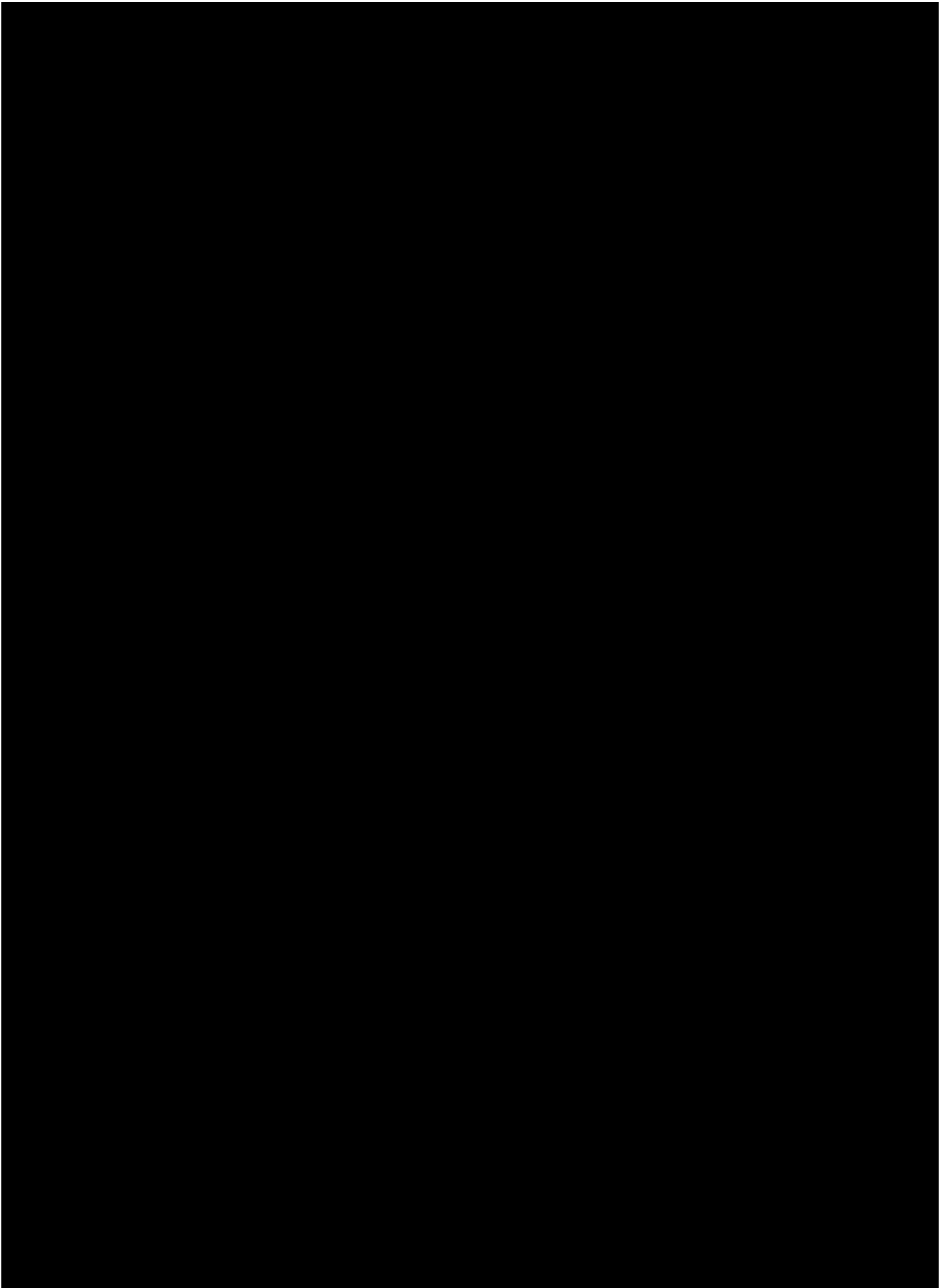
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



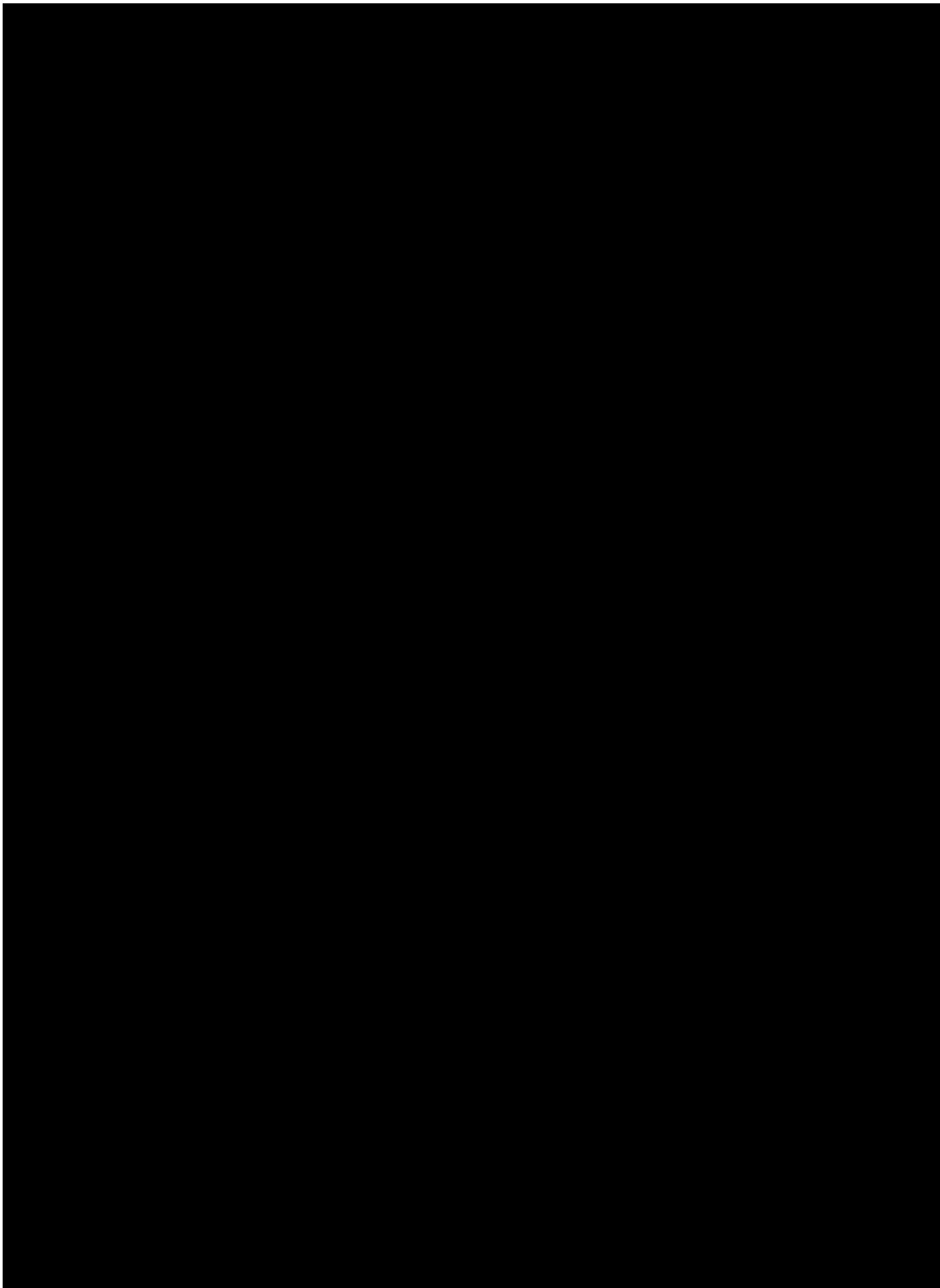
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]



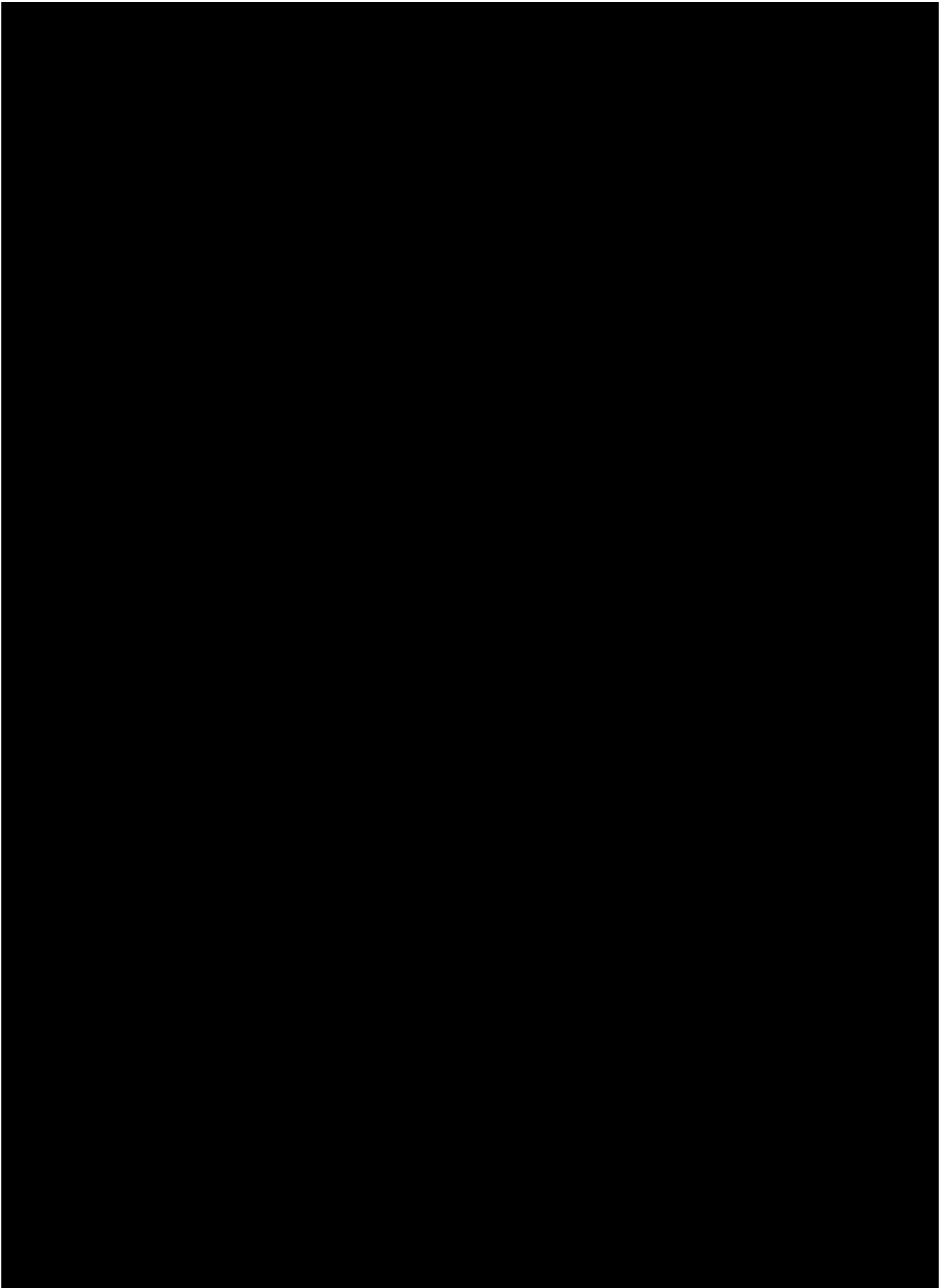
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

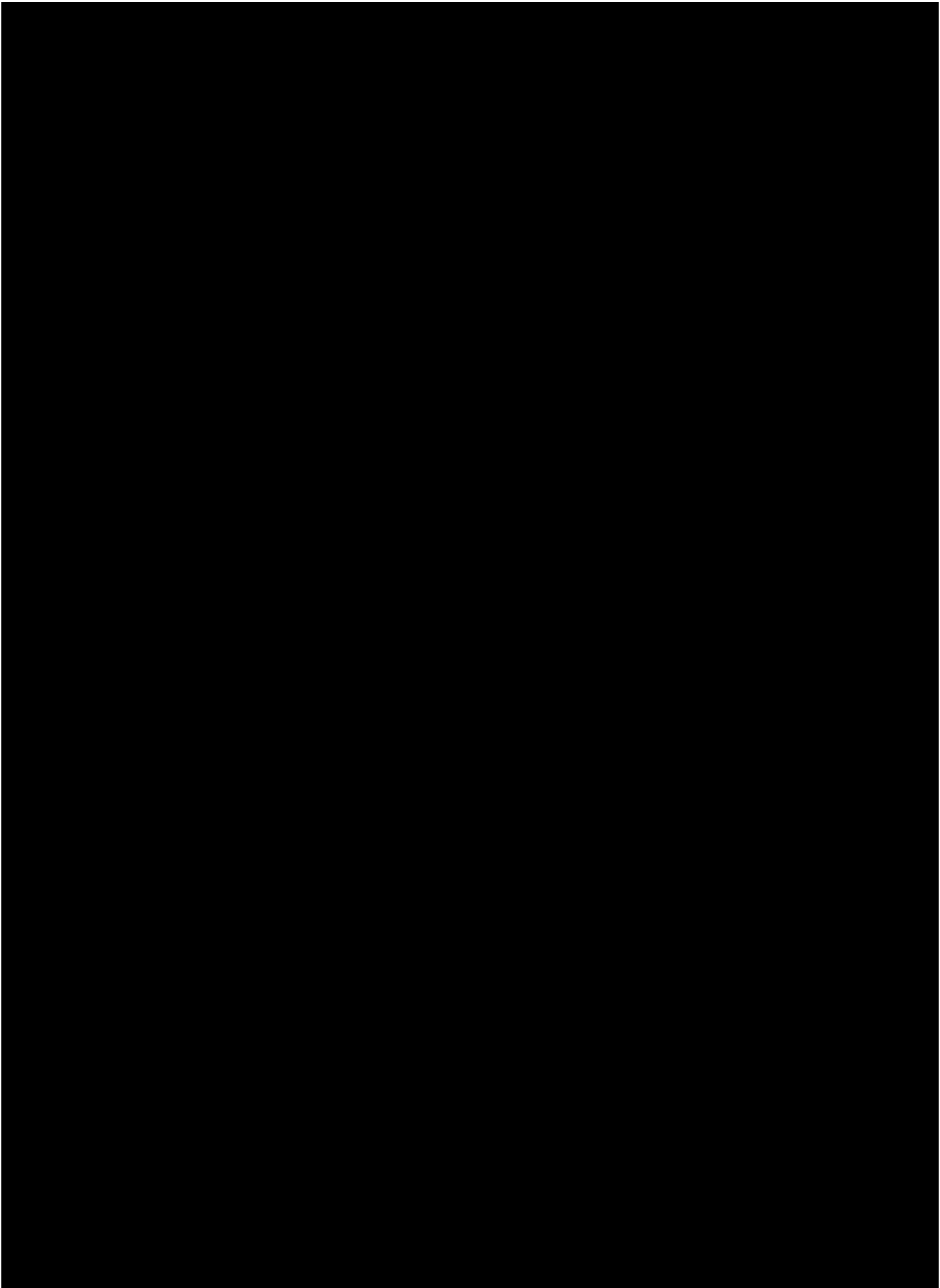
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



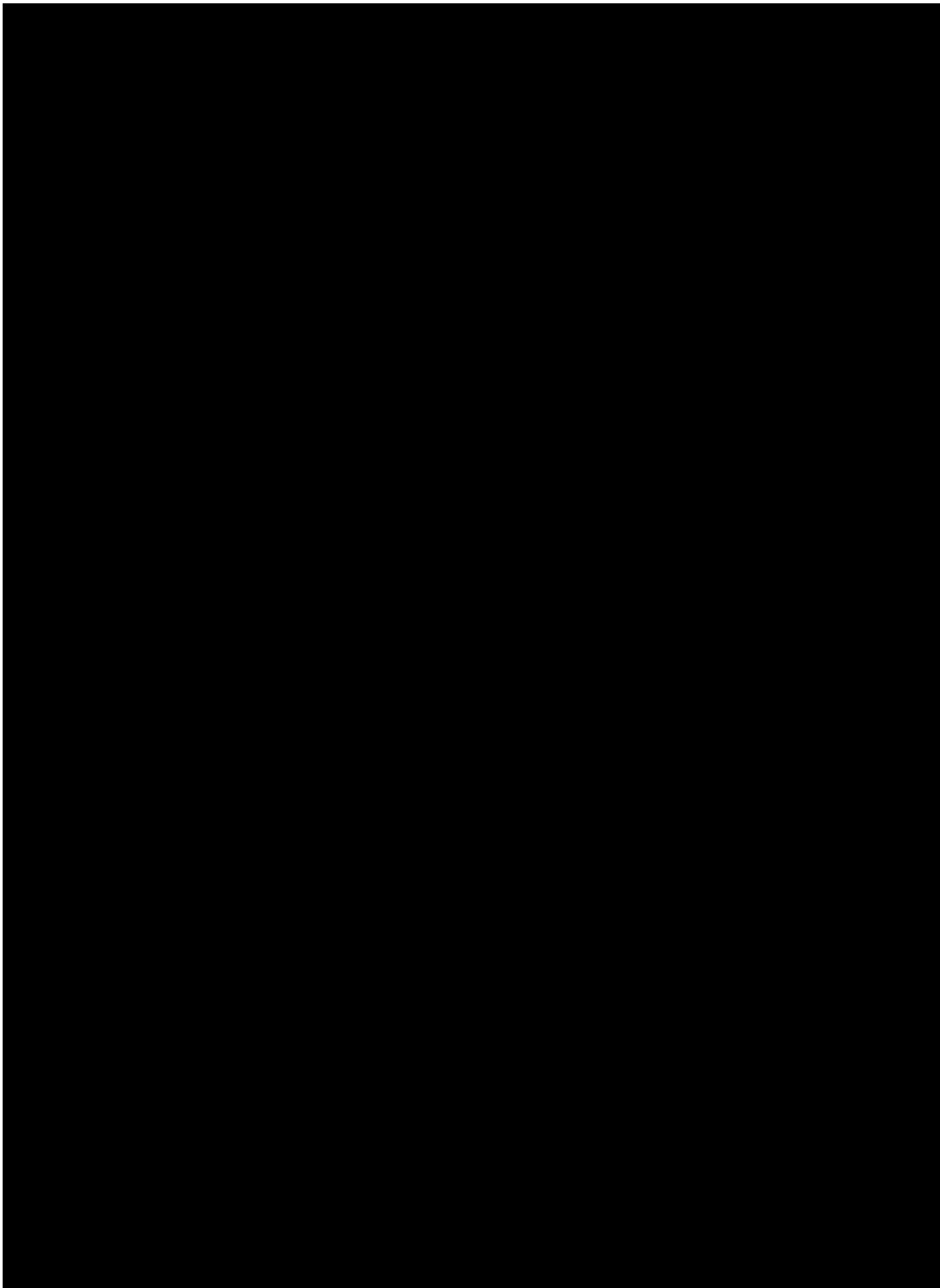
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]



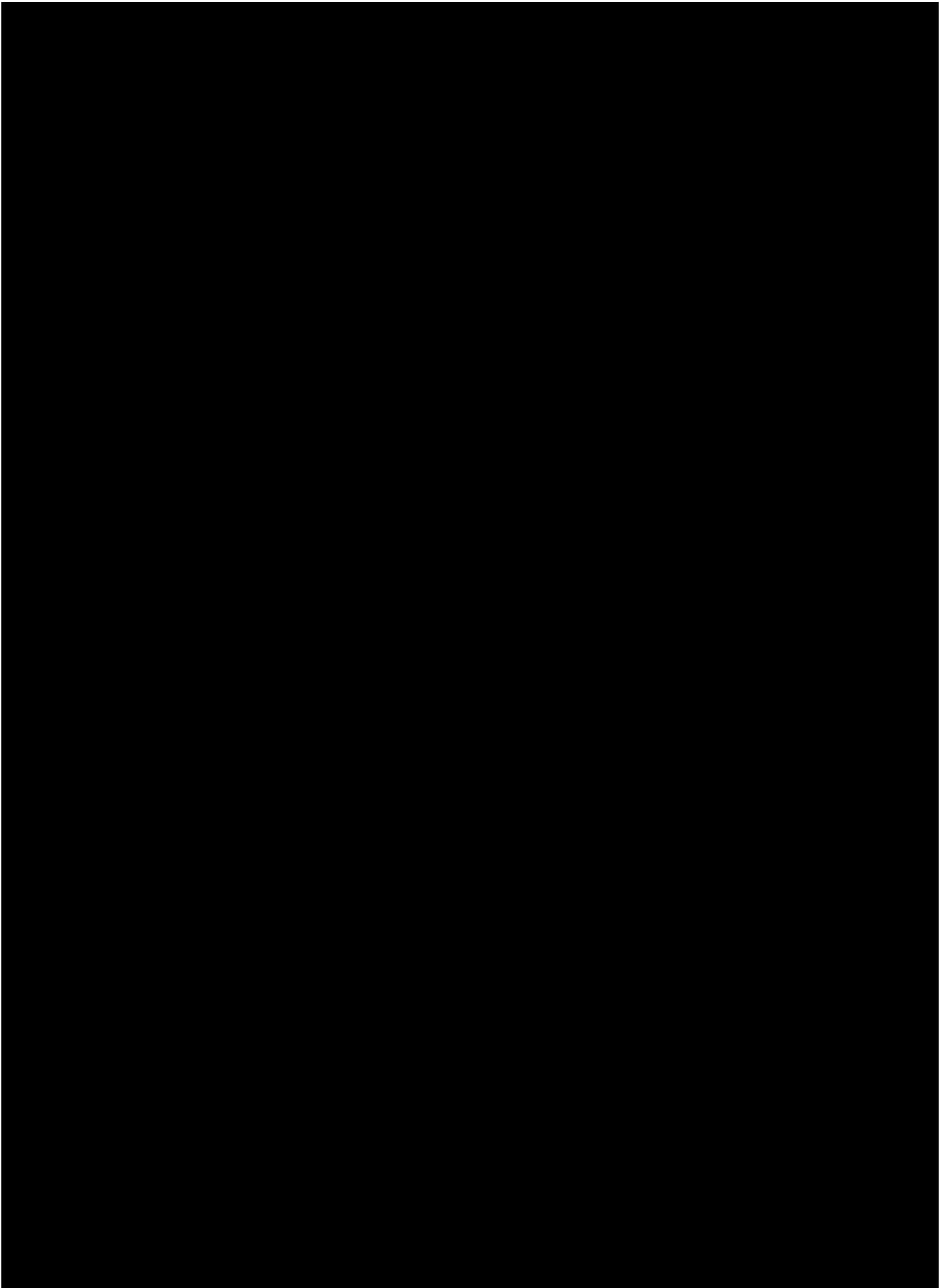
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

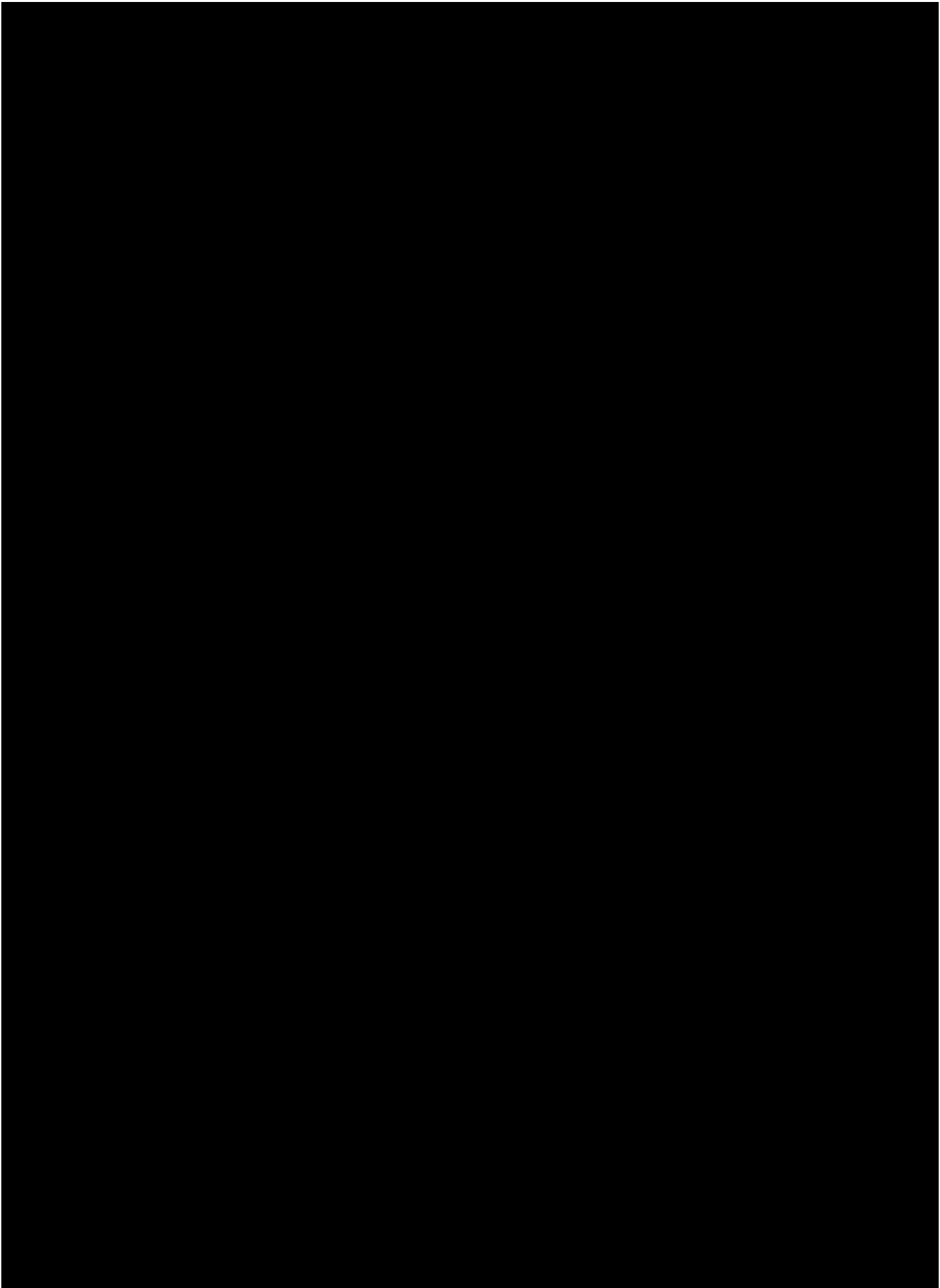
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

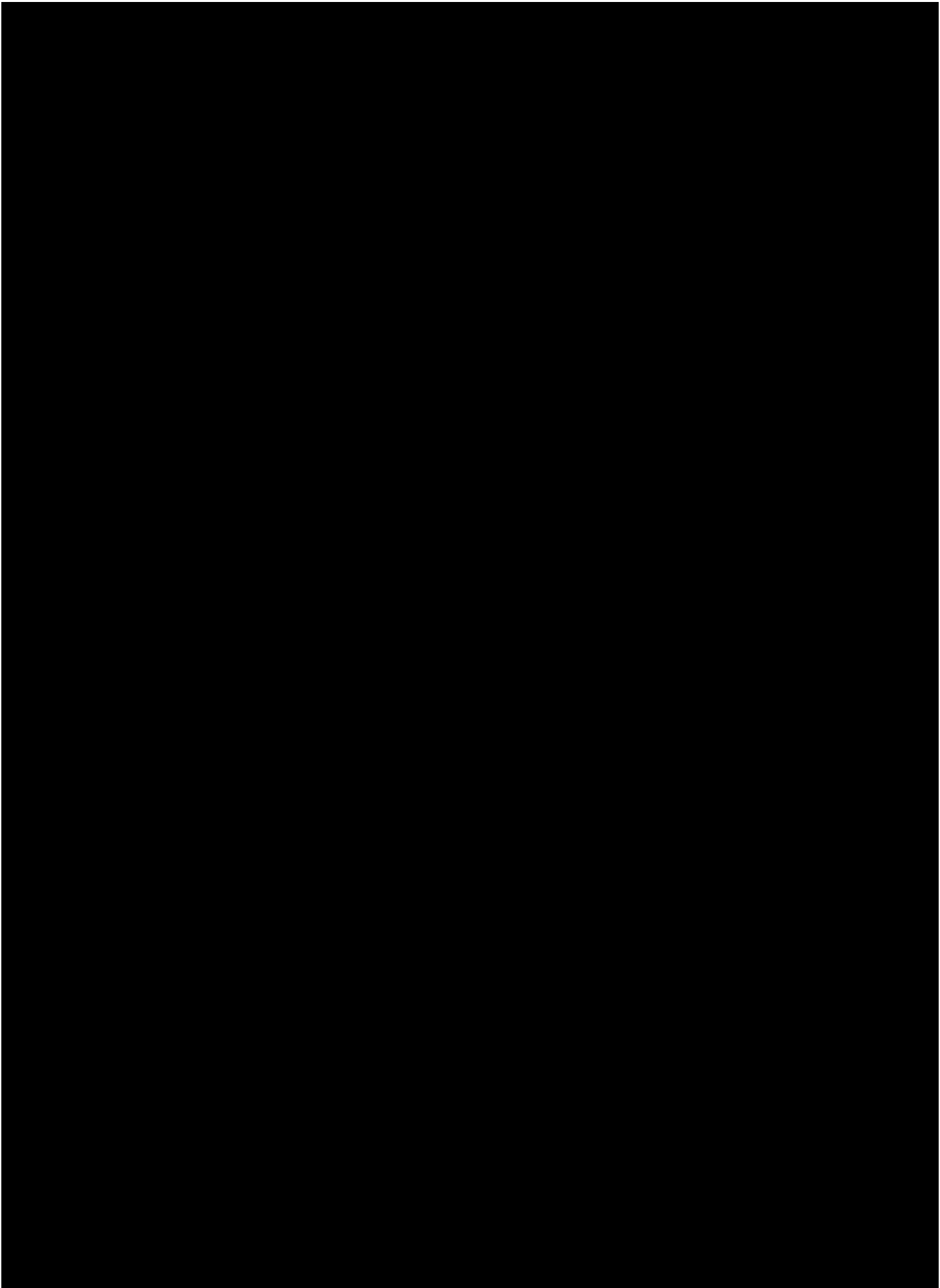
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

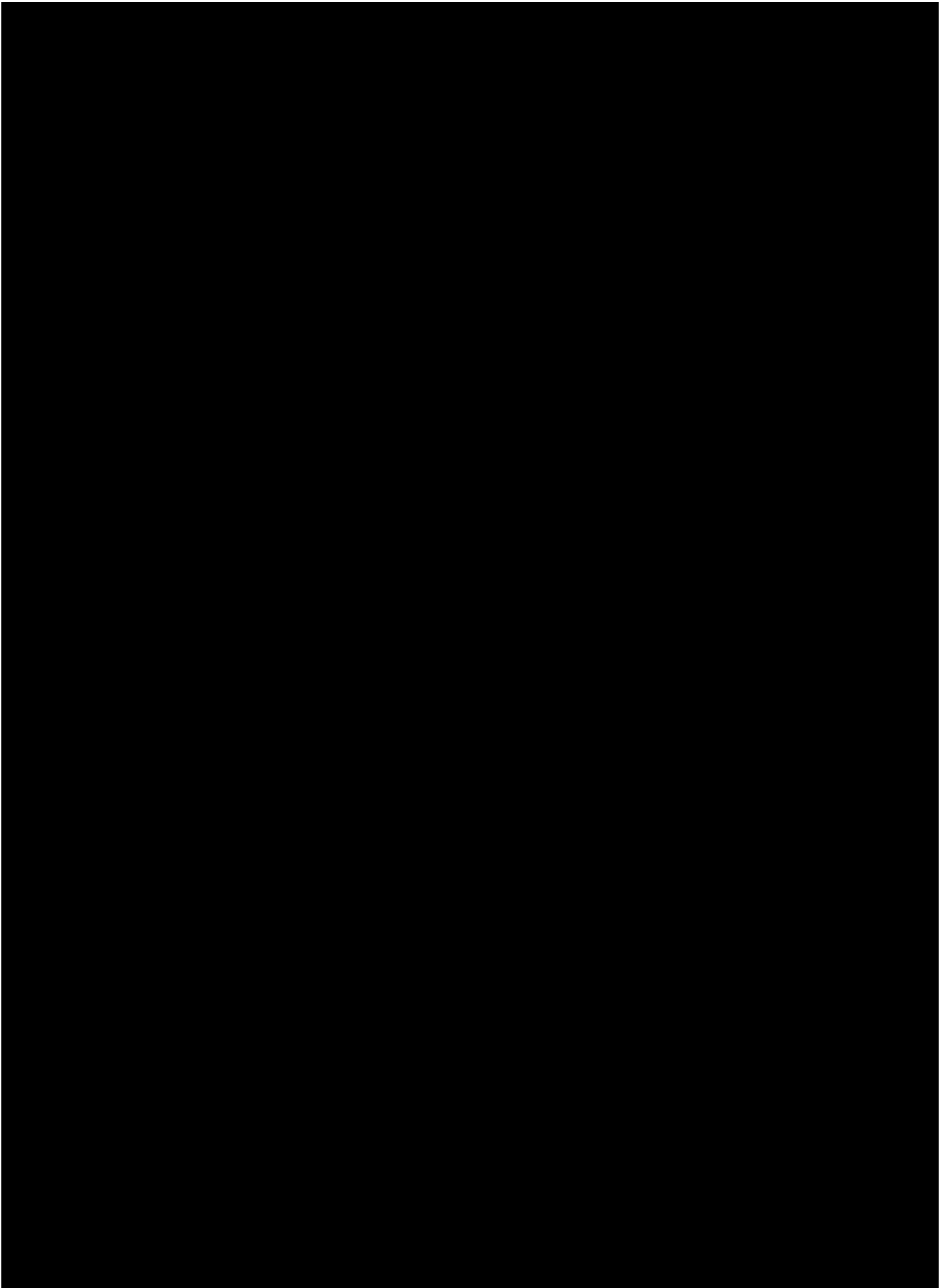
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

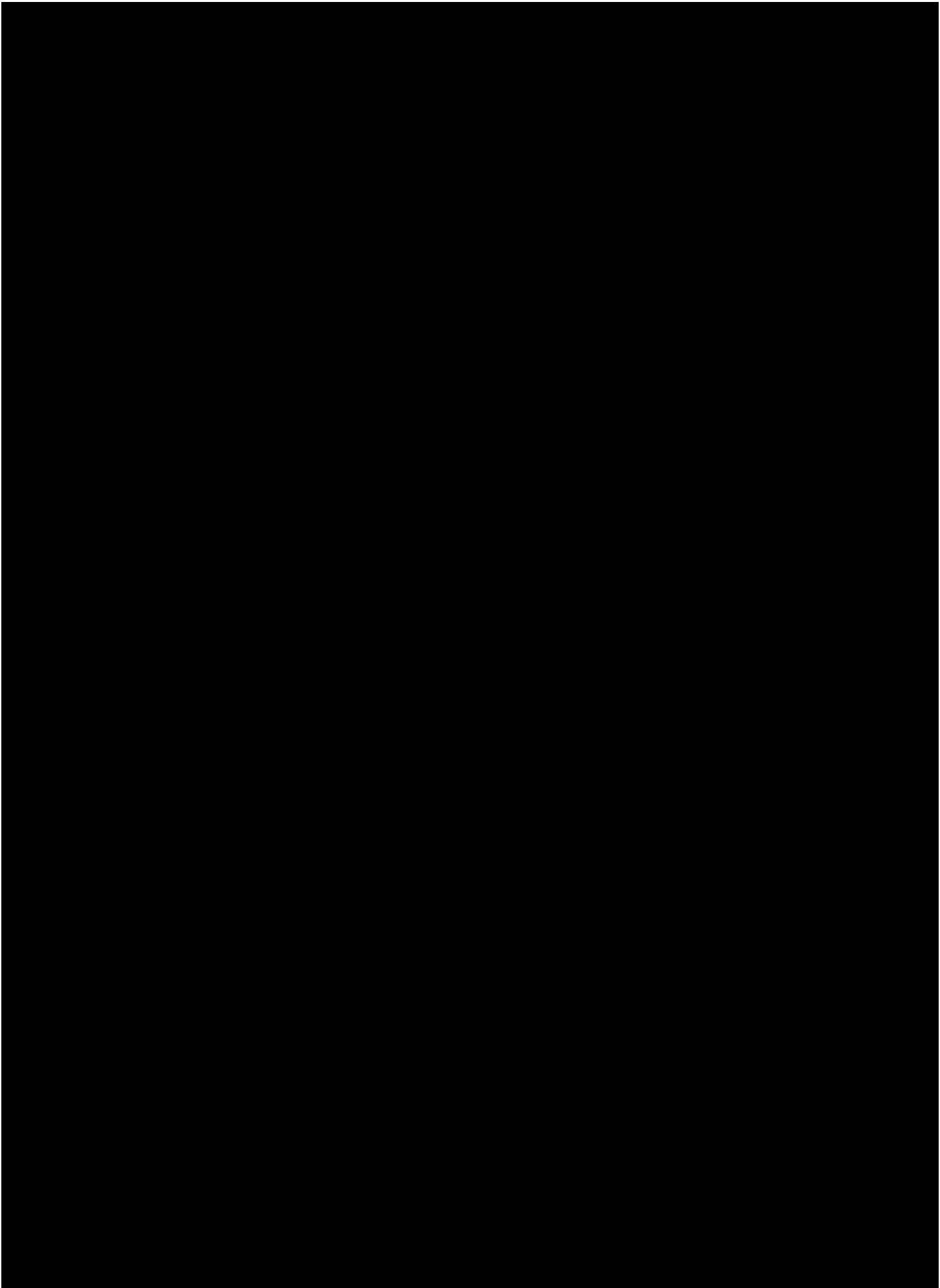
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

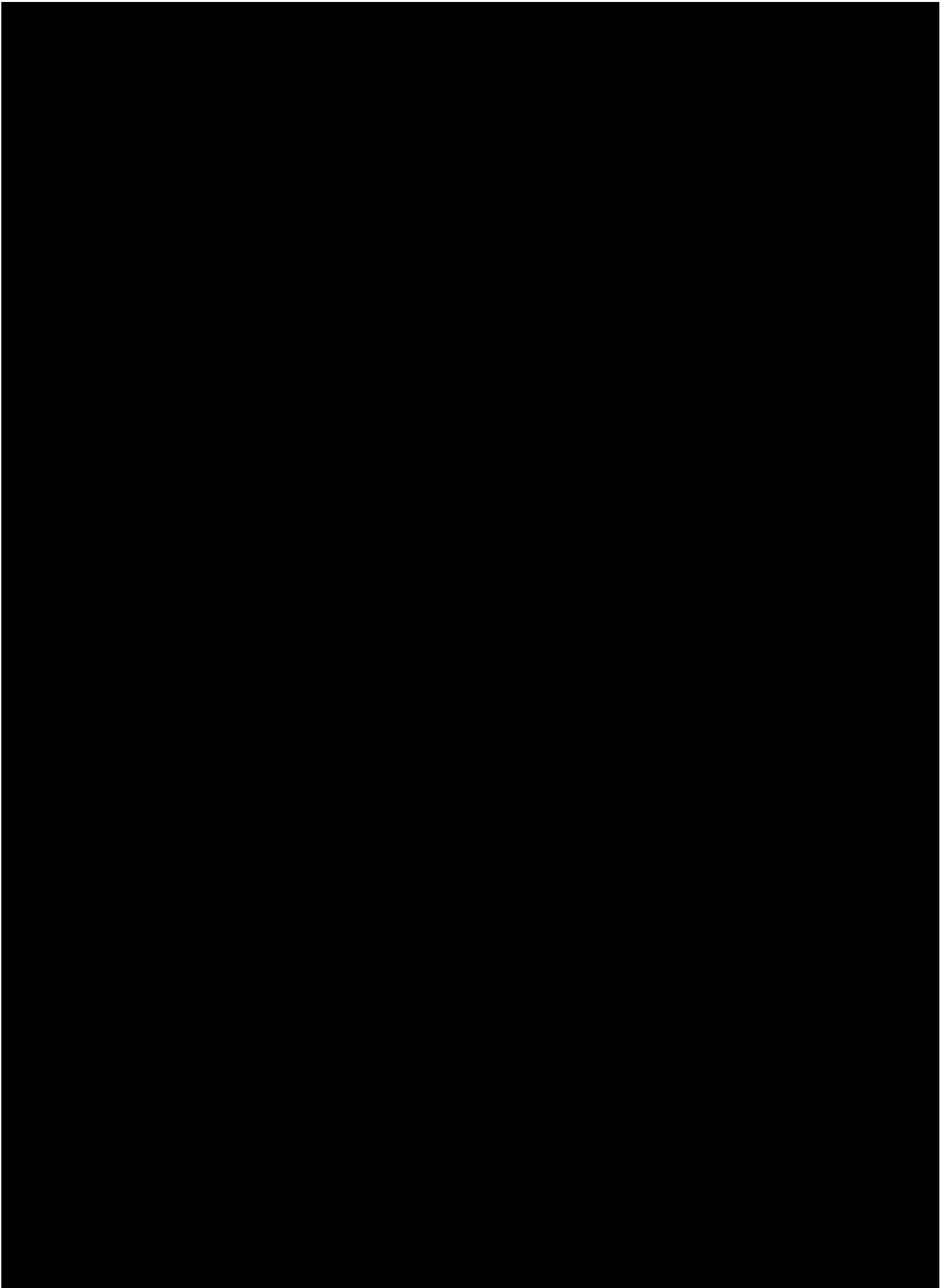
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

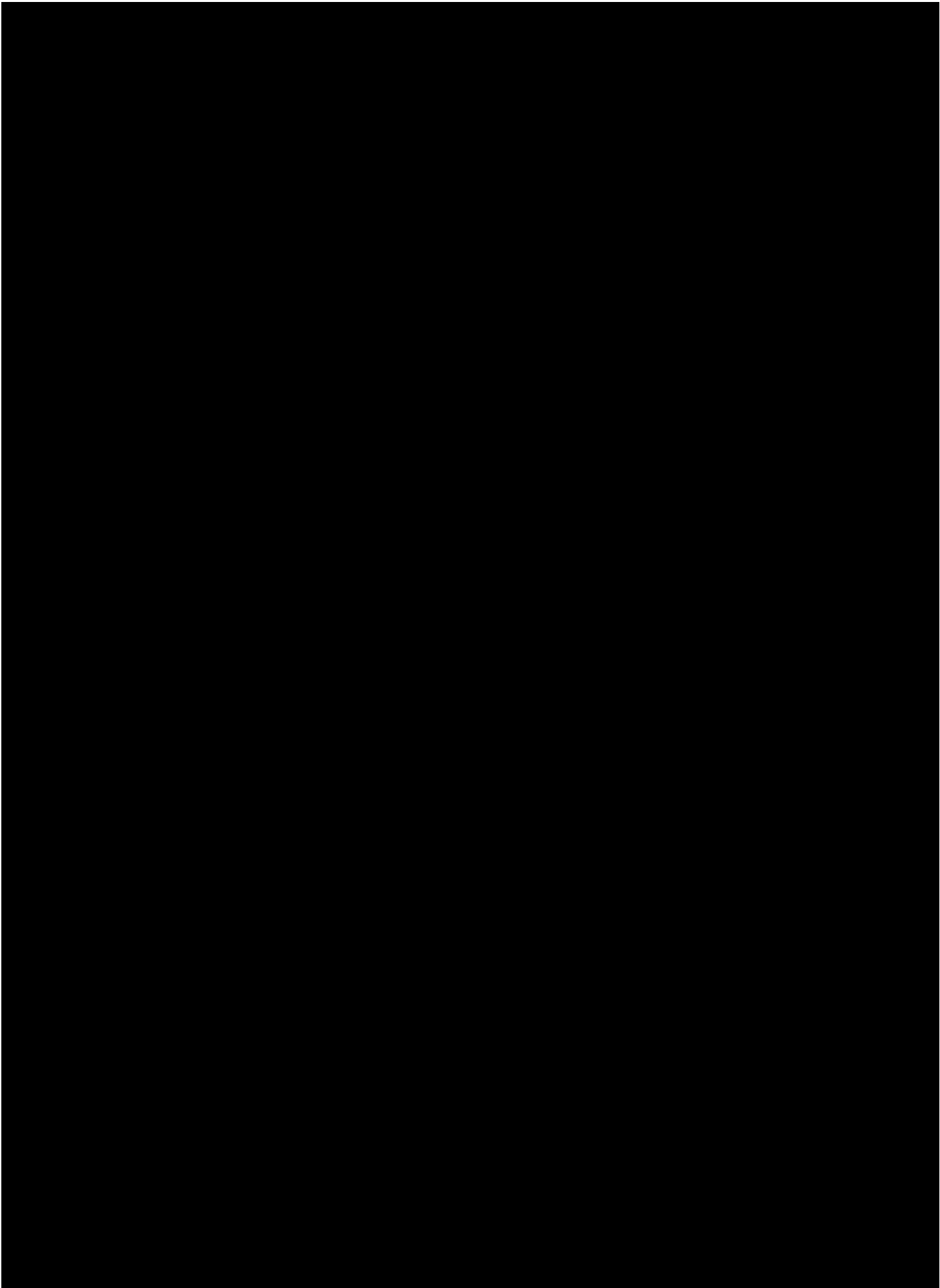
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



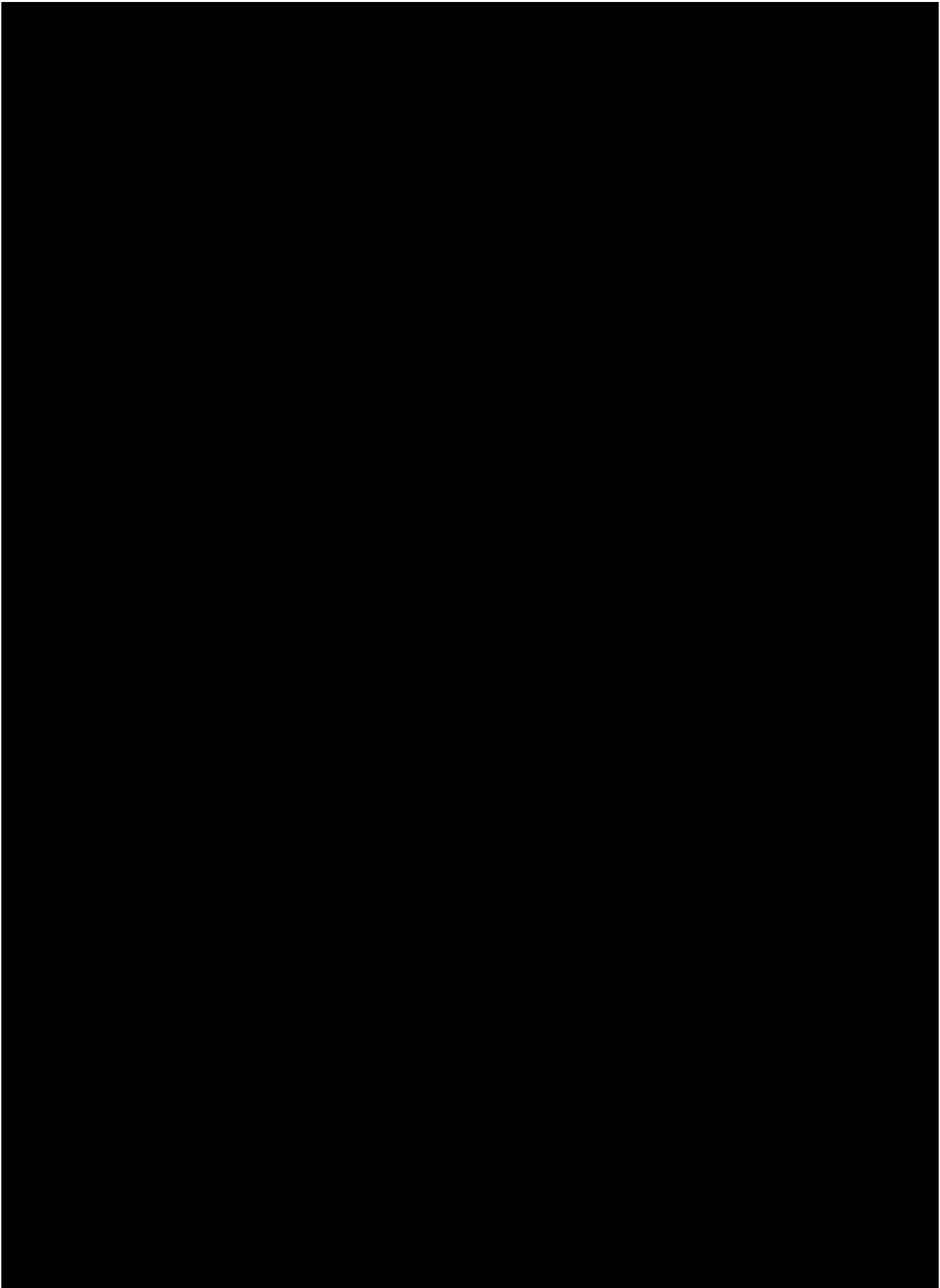
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

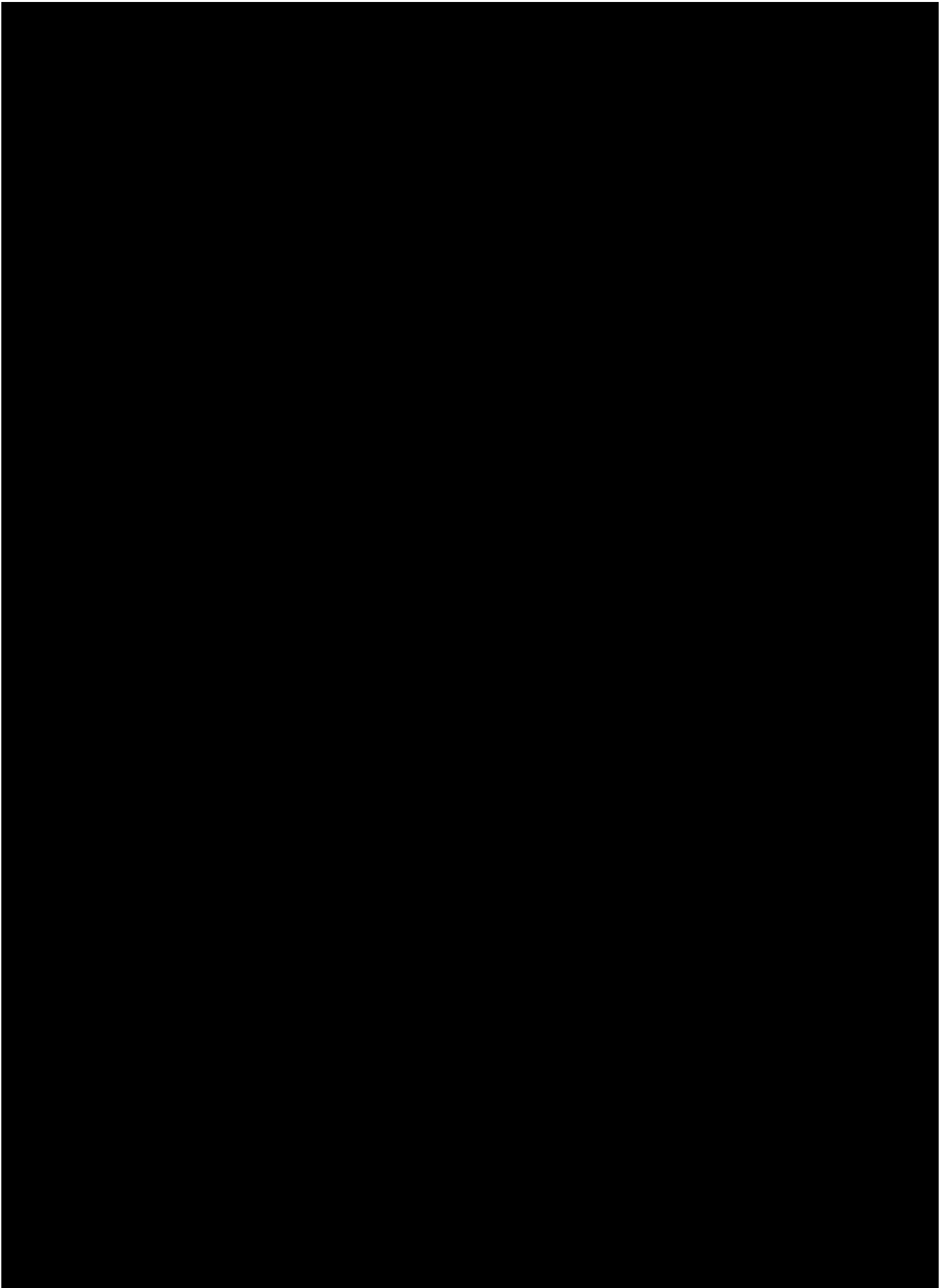
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



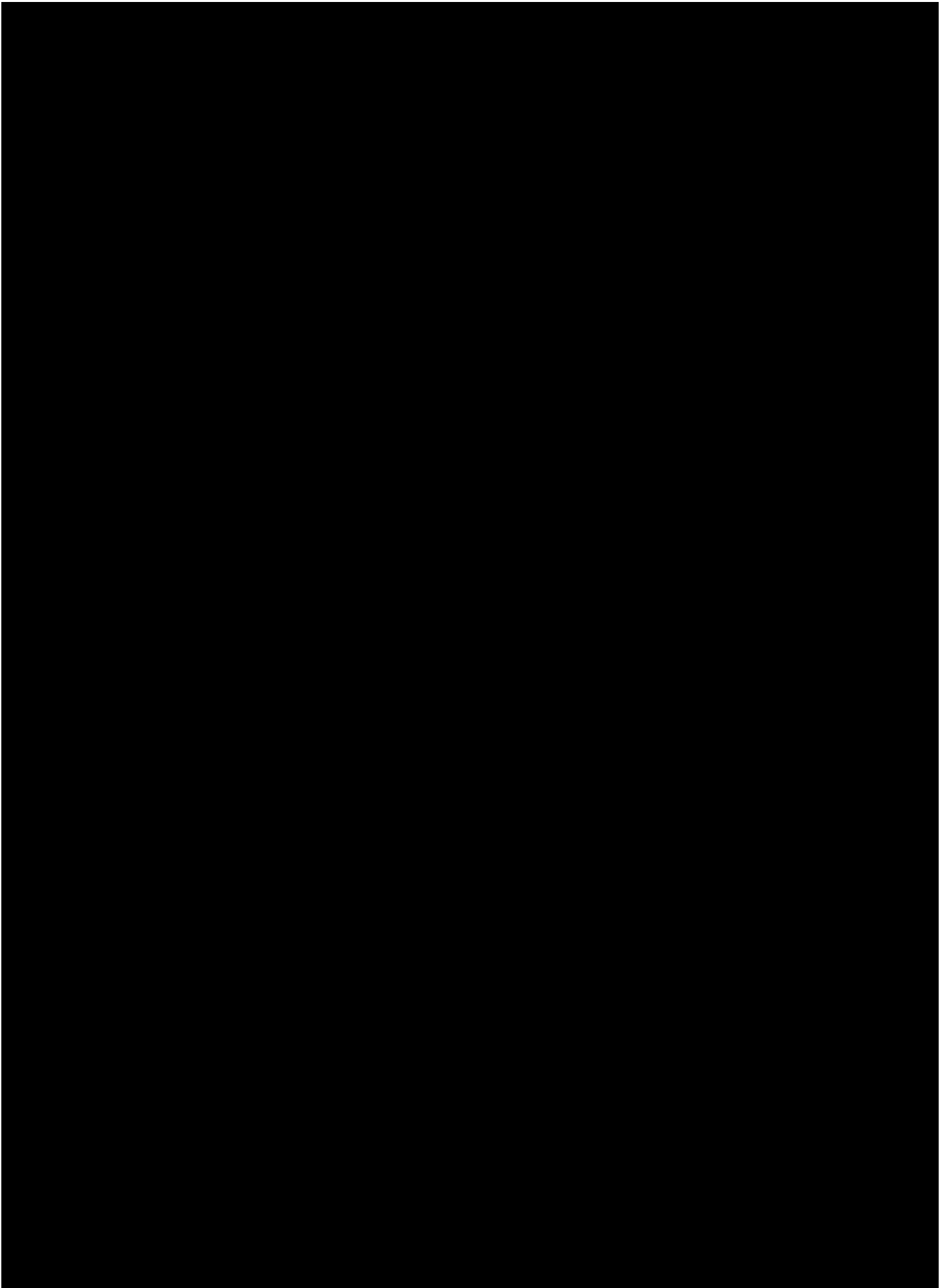
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

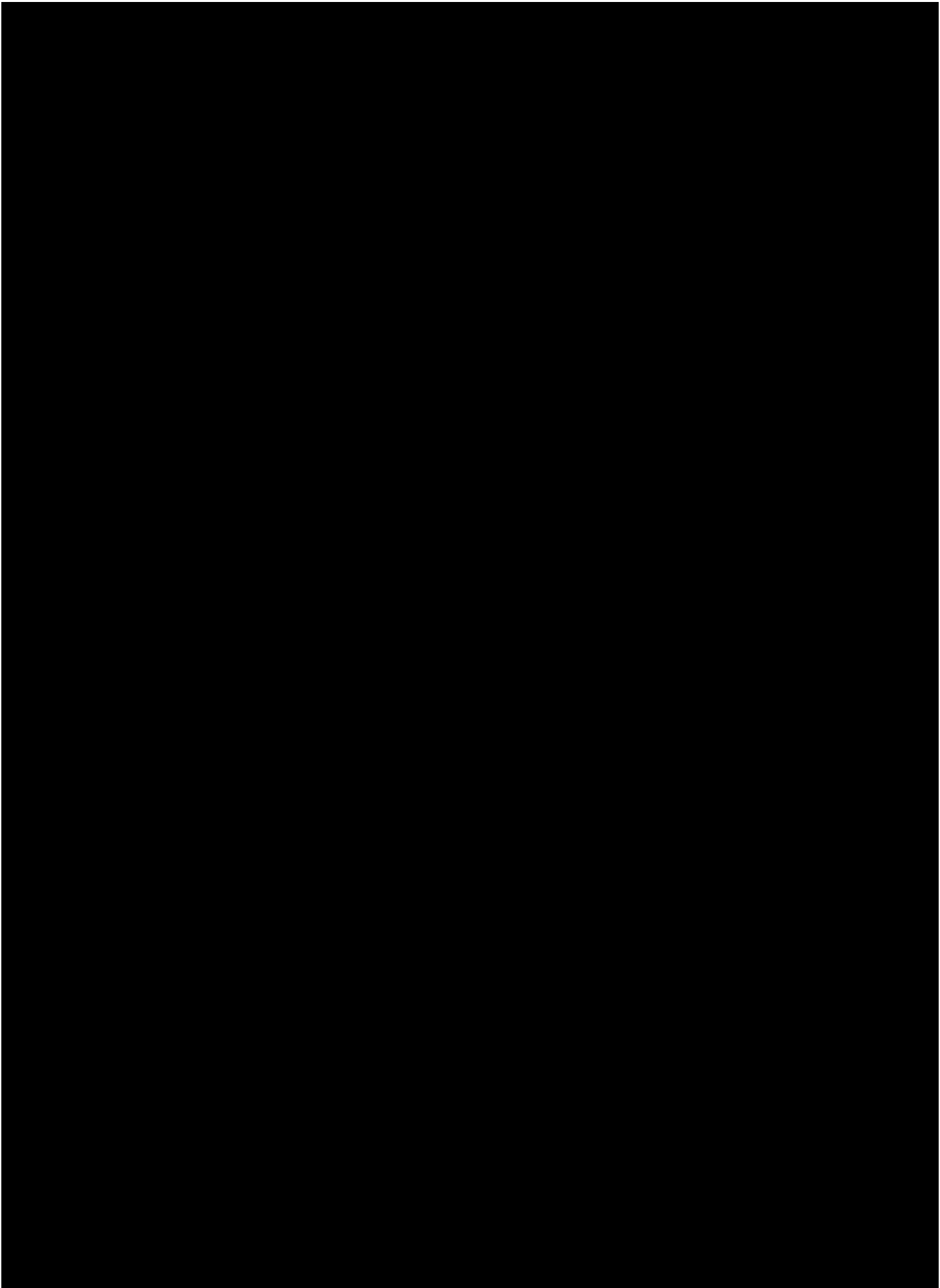
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



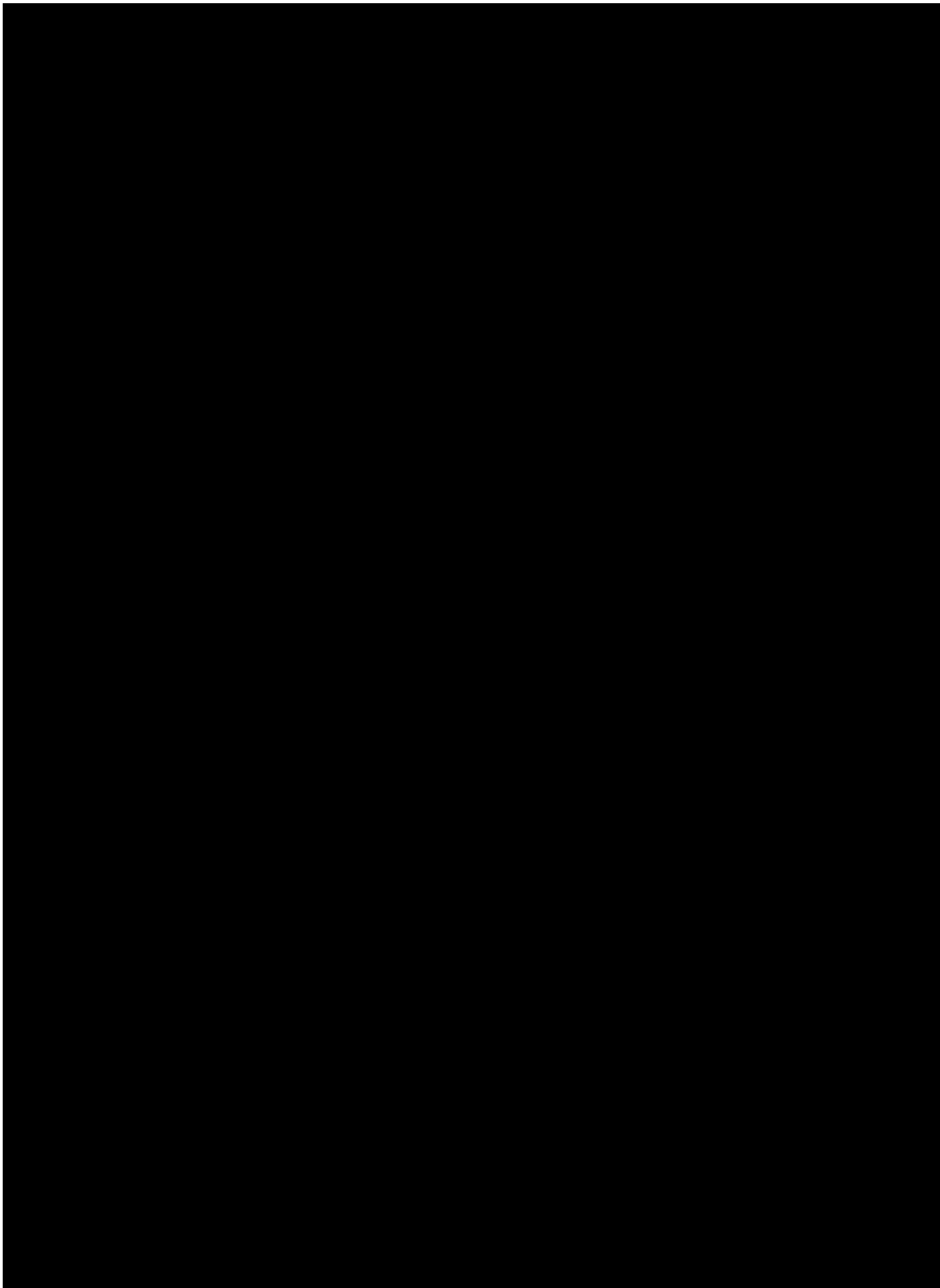
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

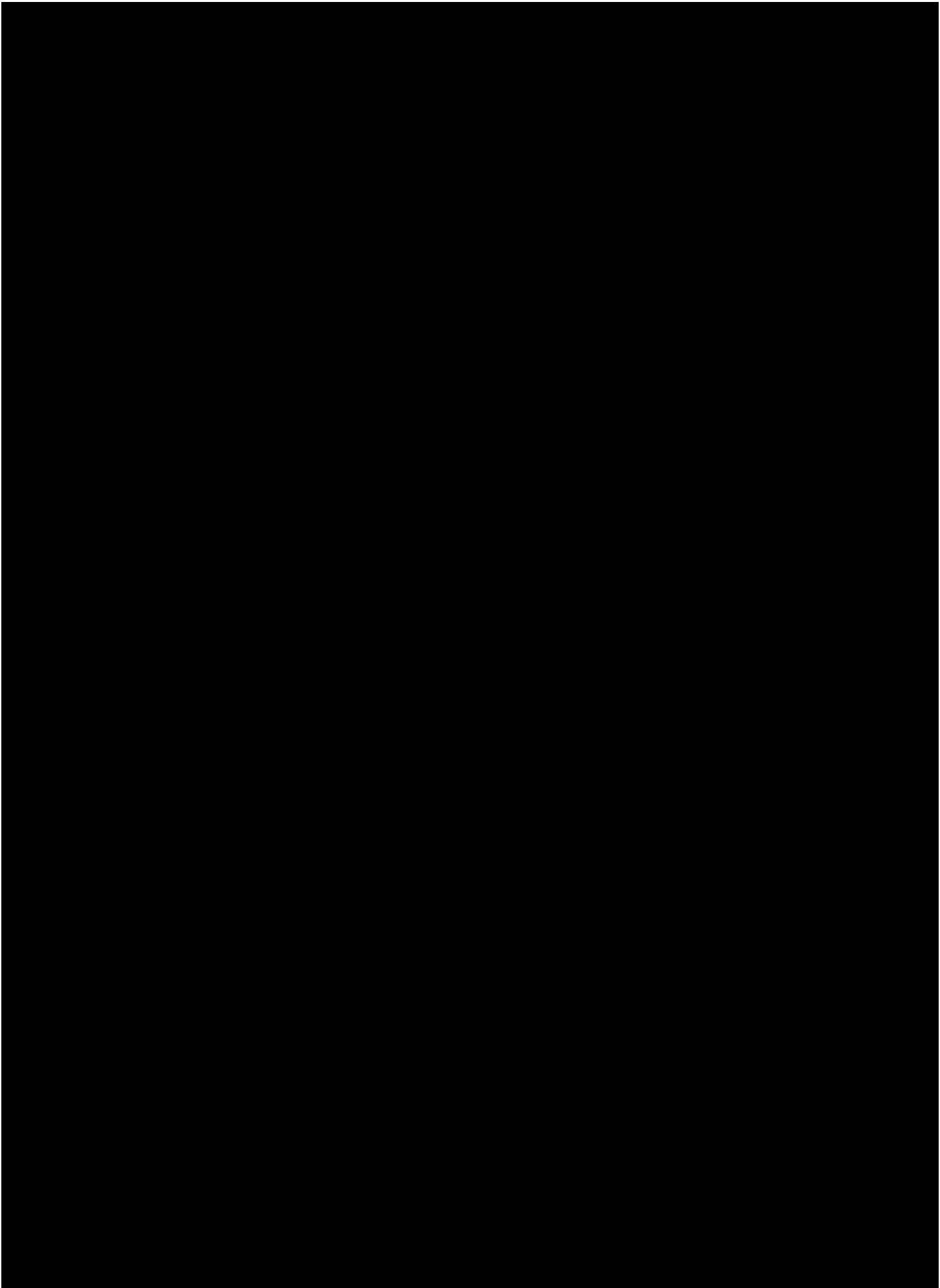
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

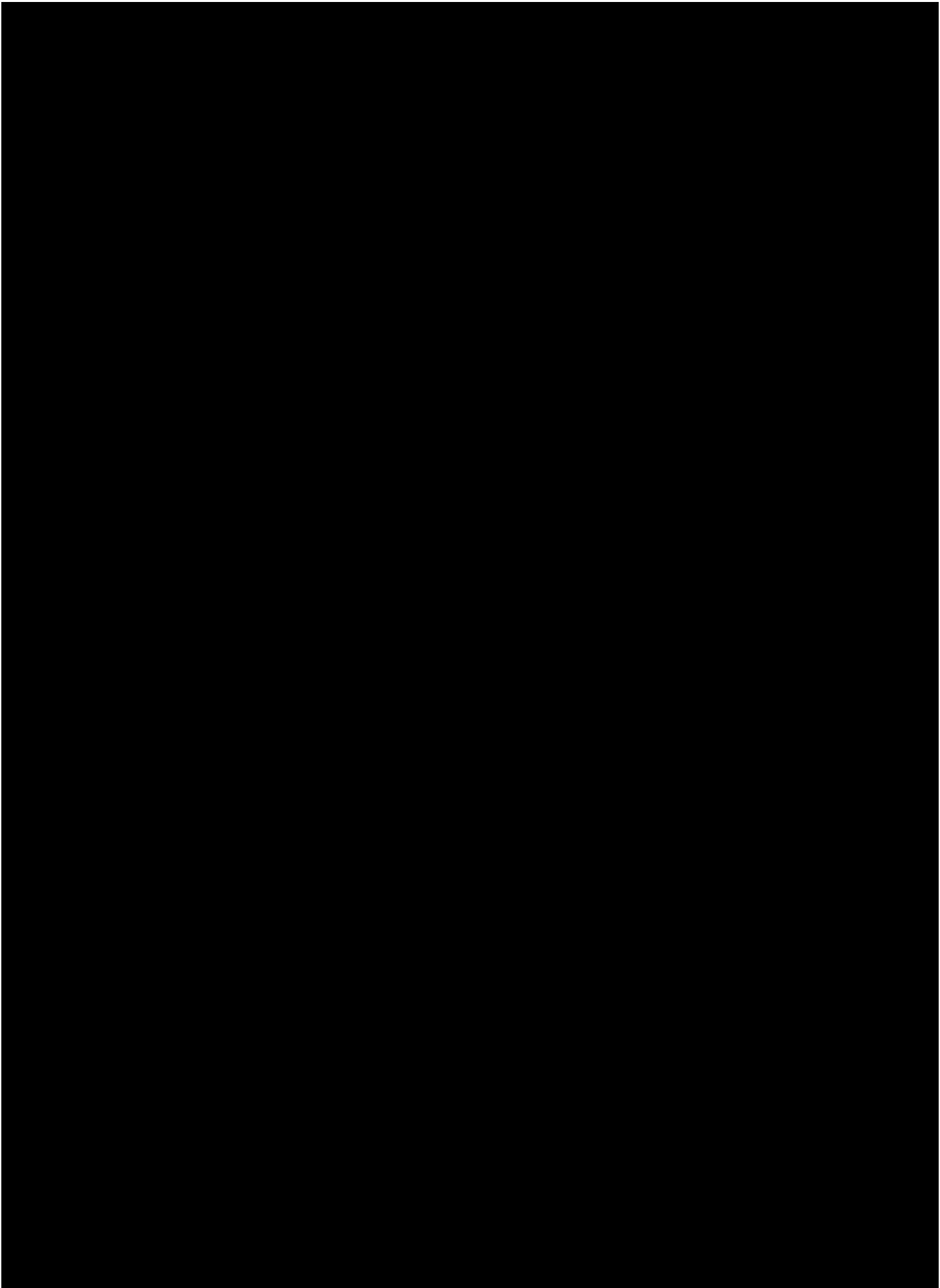
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

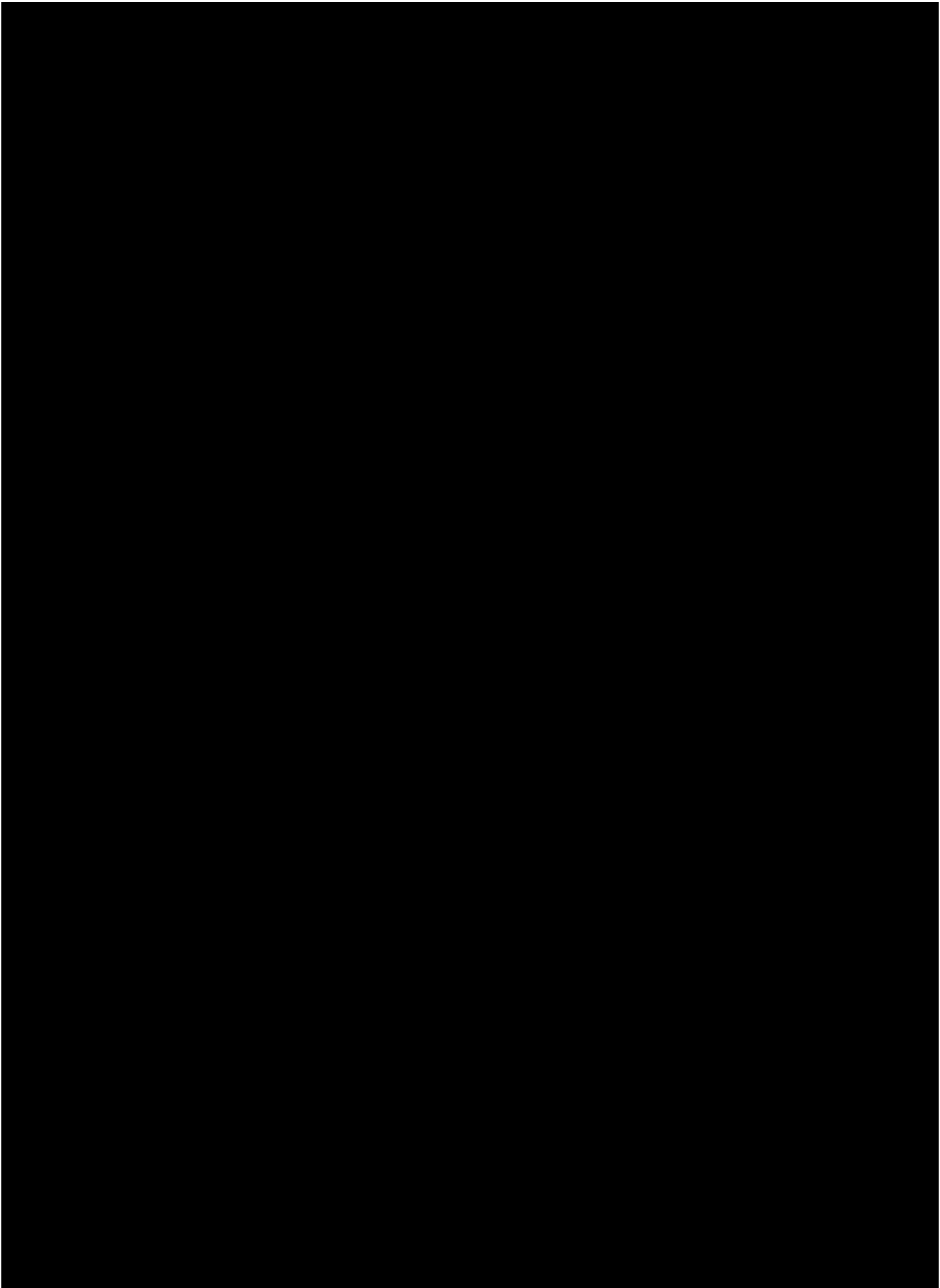
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

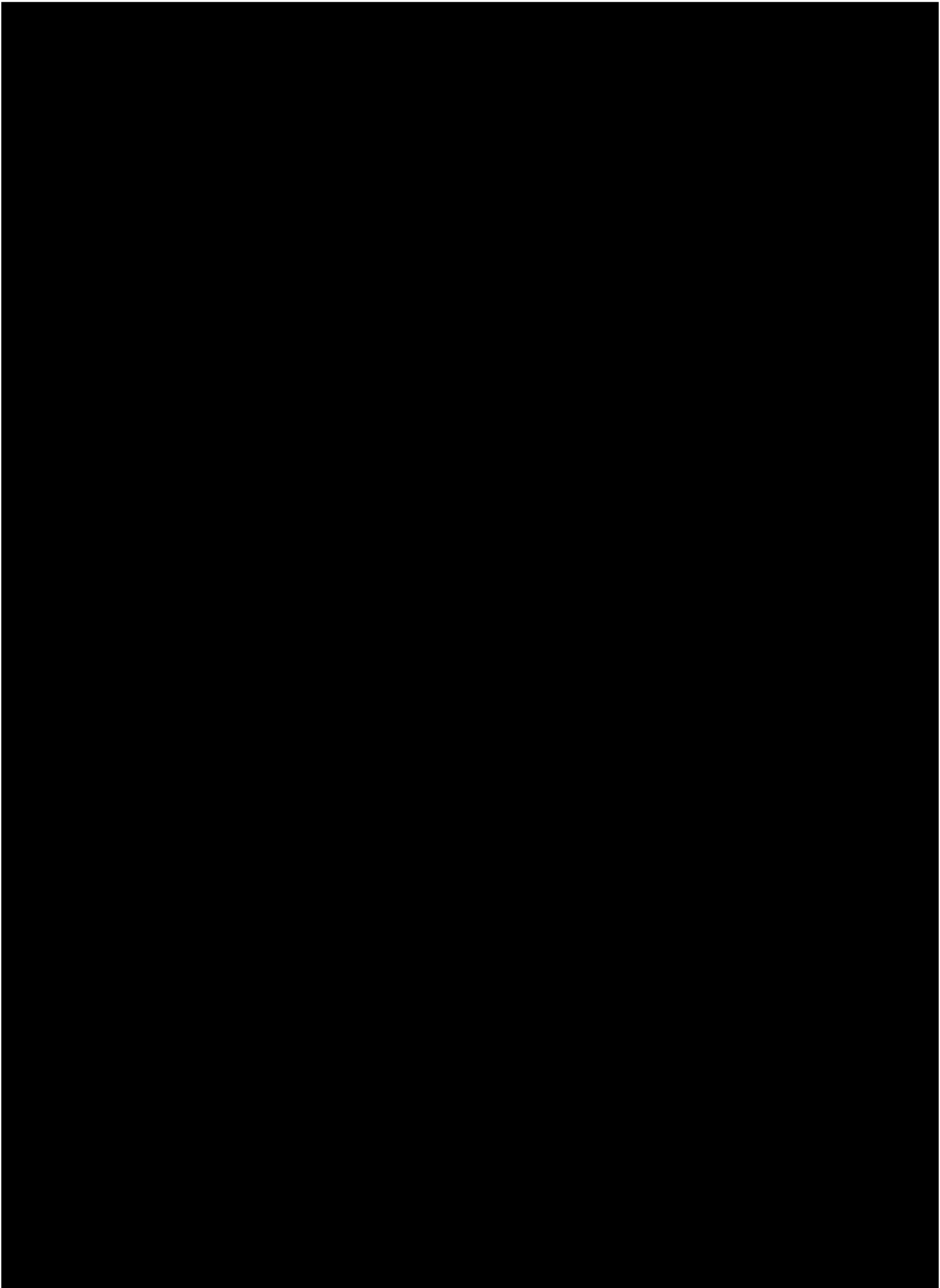
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



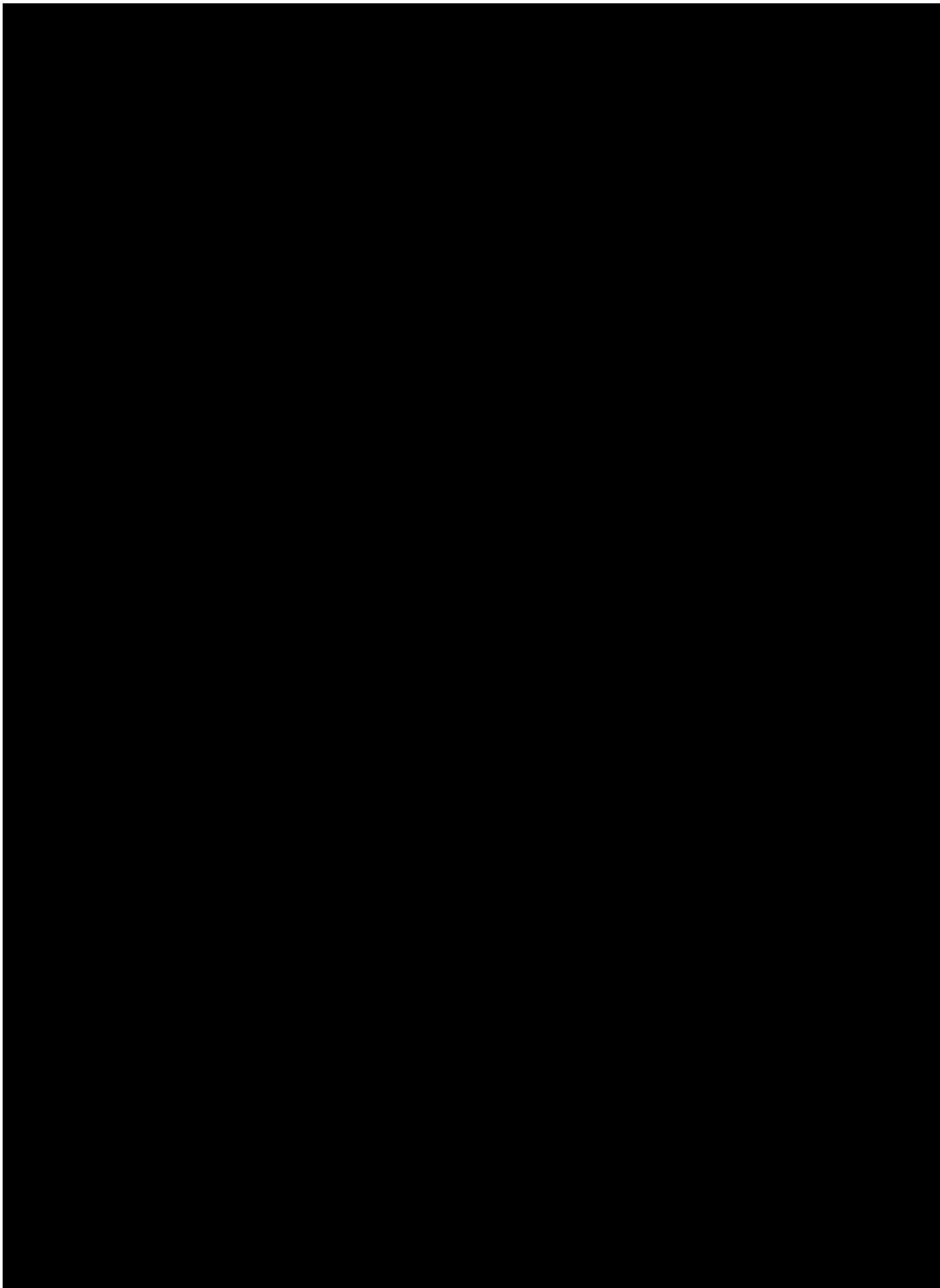
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

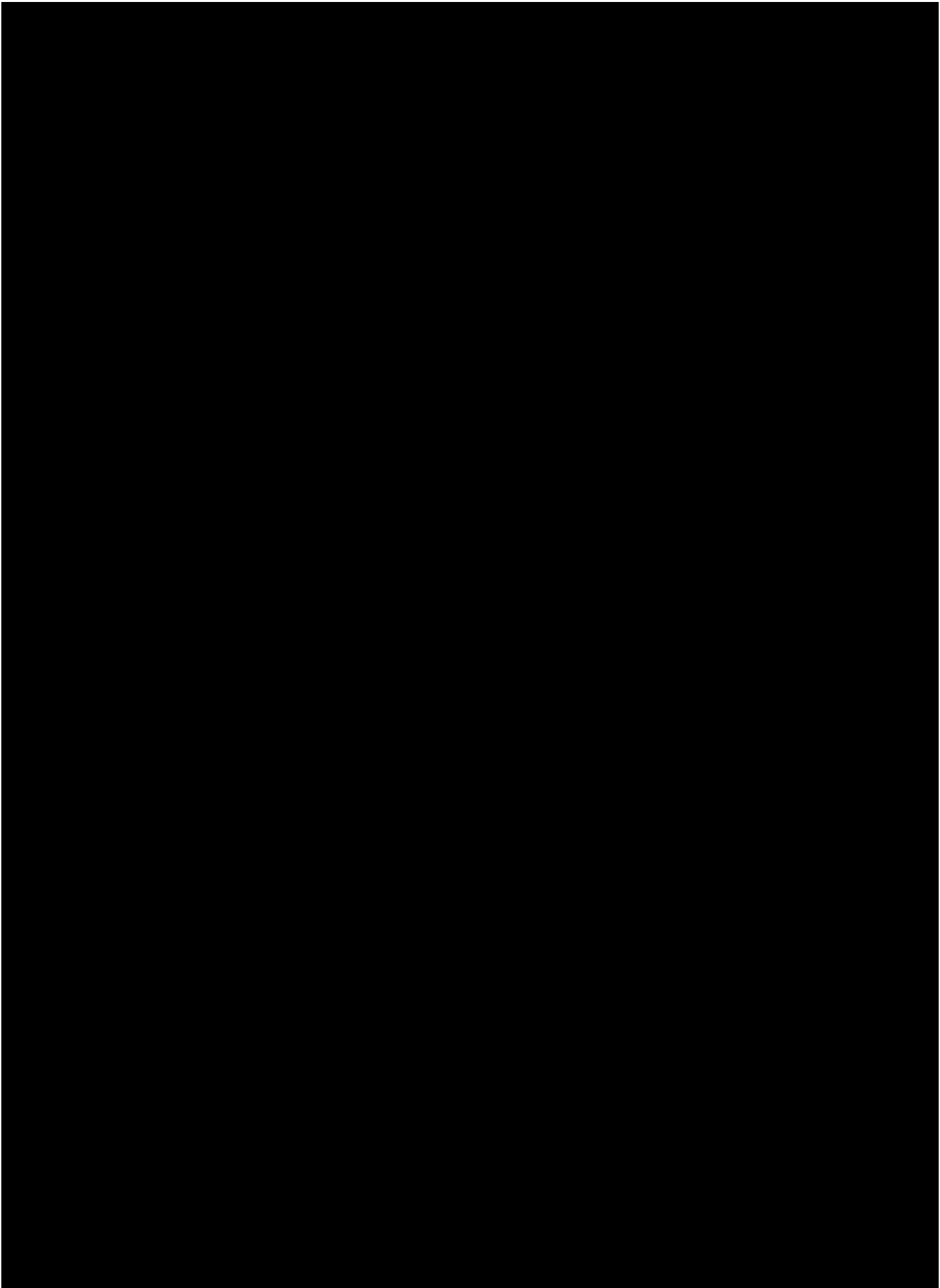
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



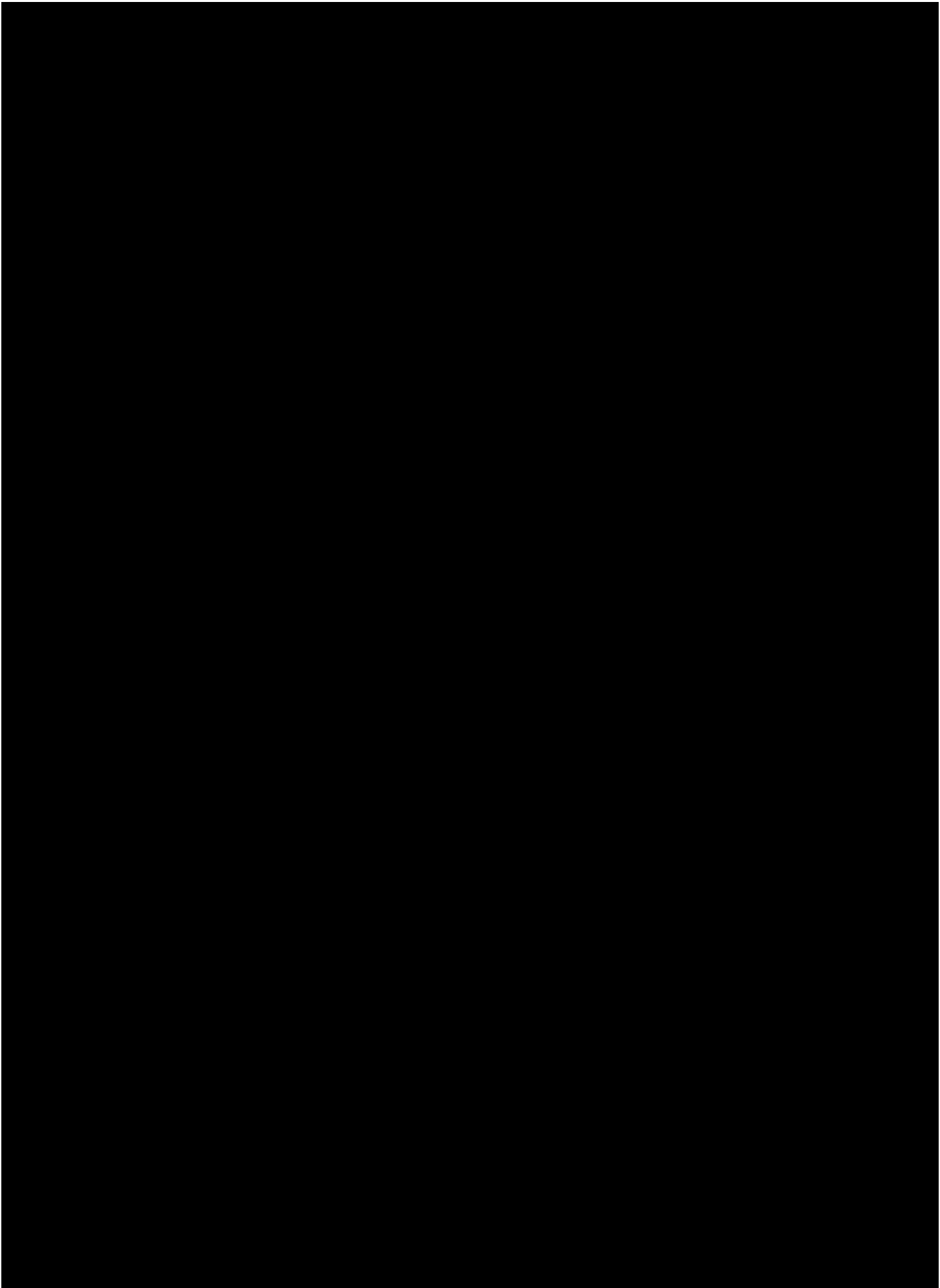
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]



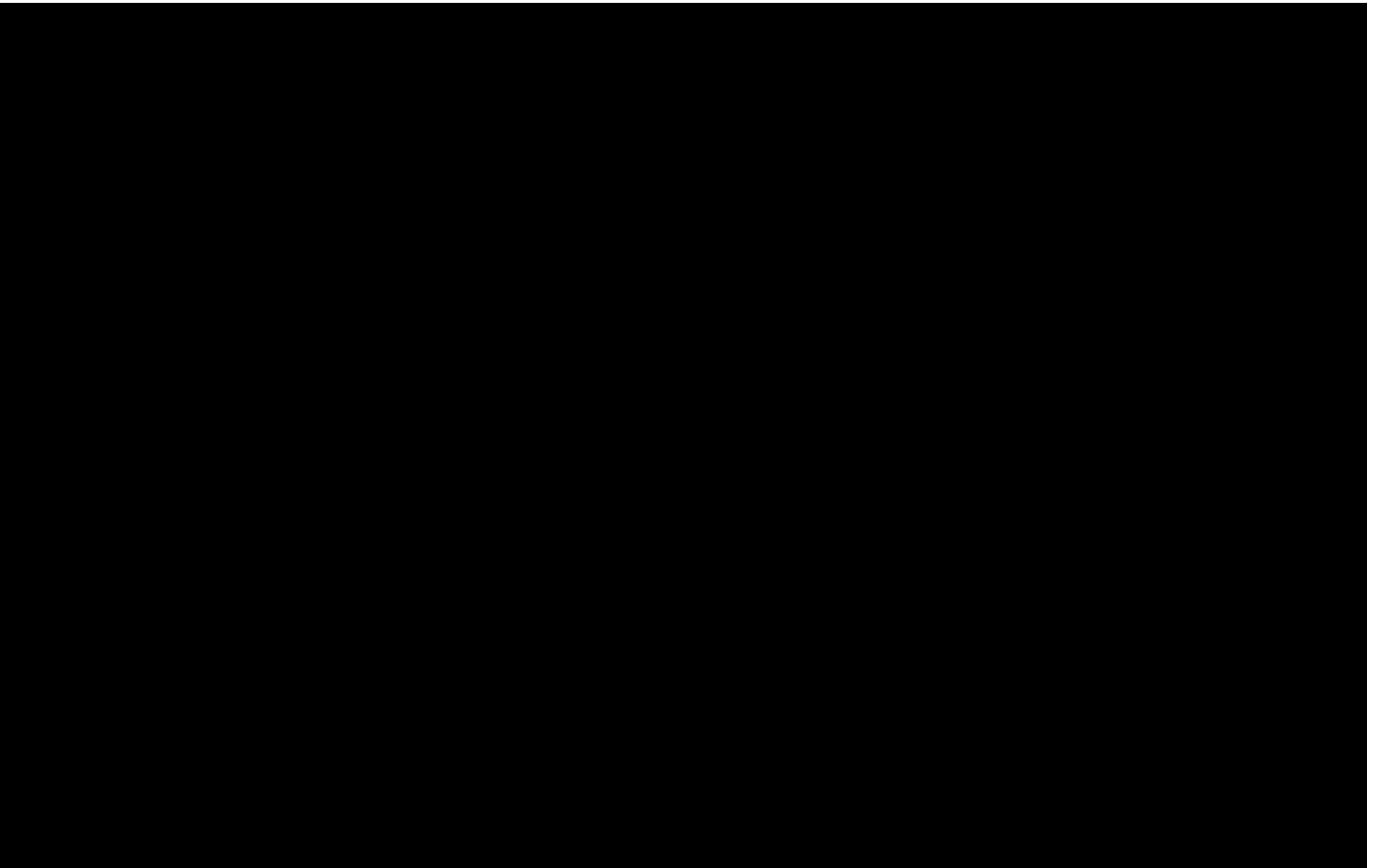
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

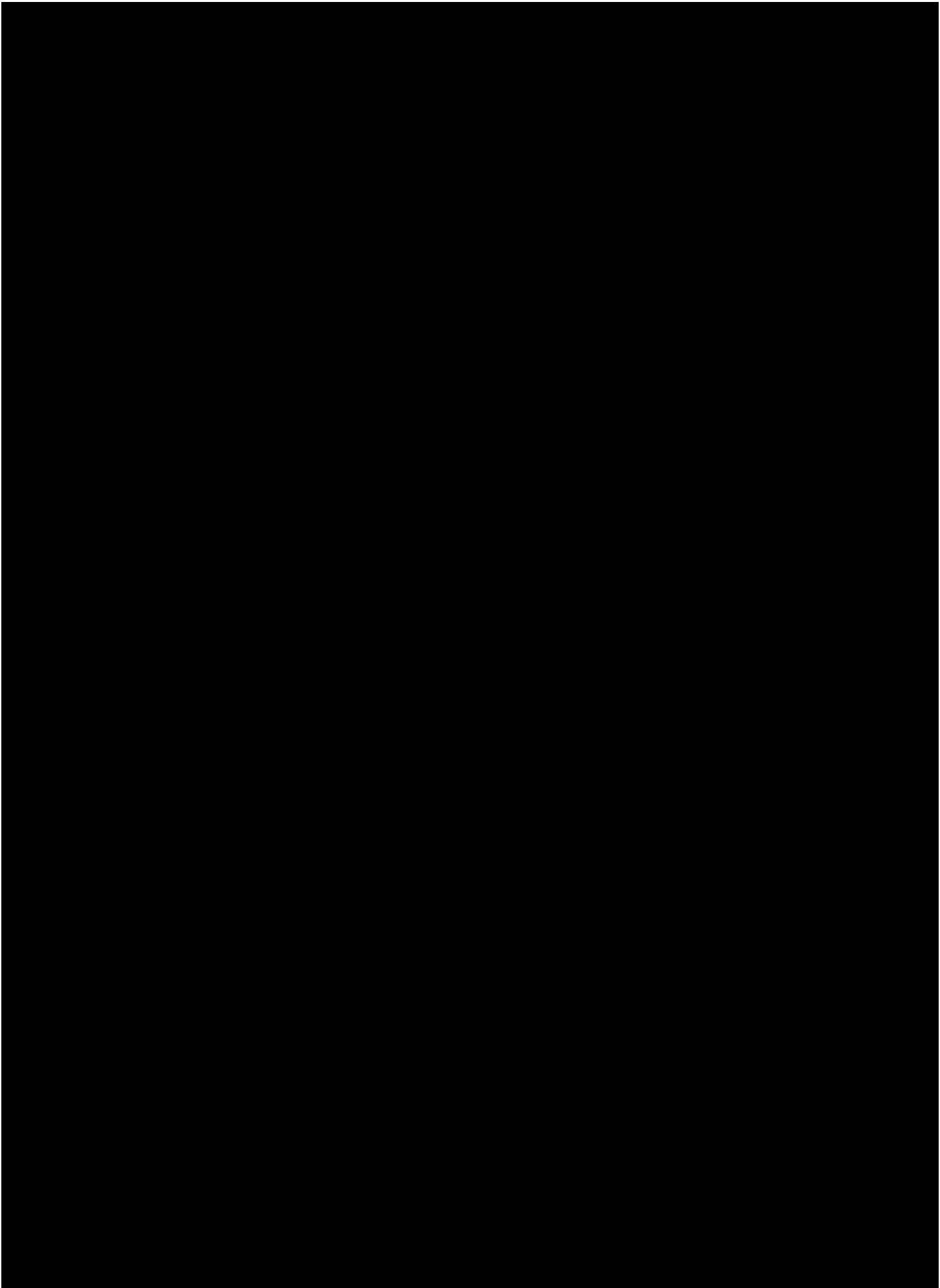
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

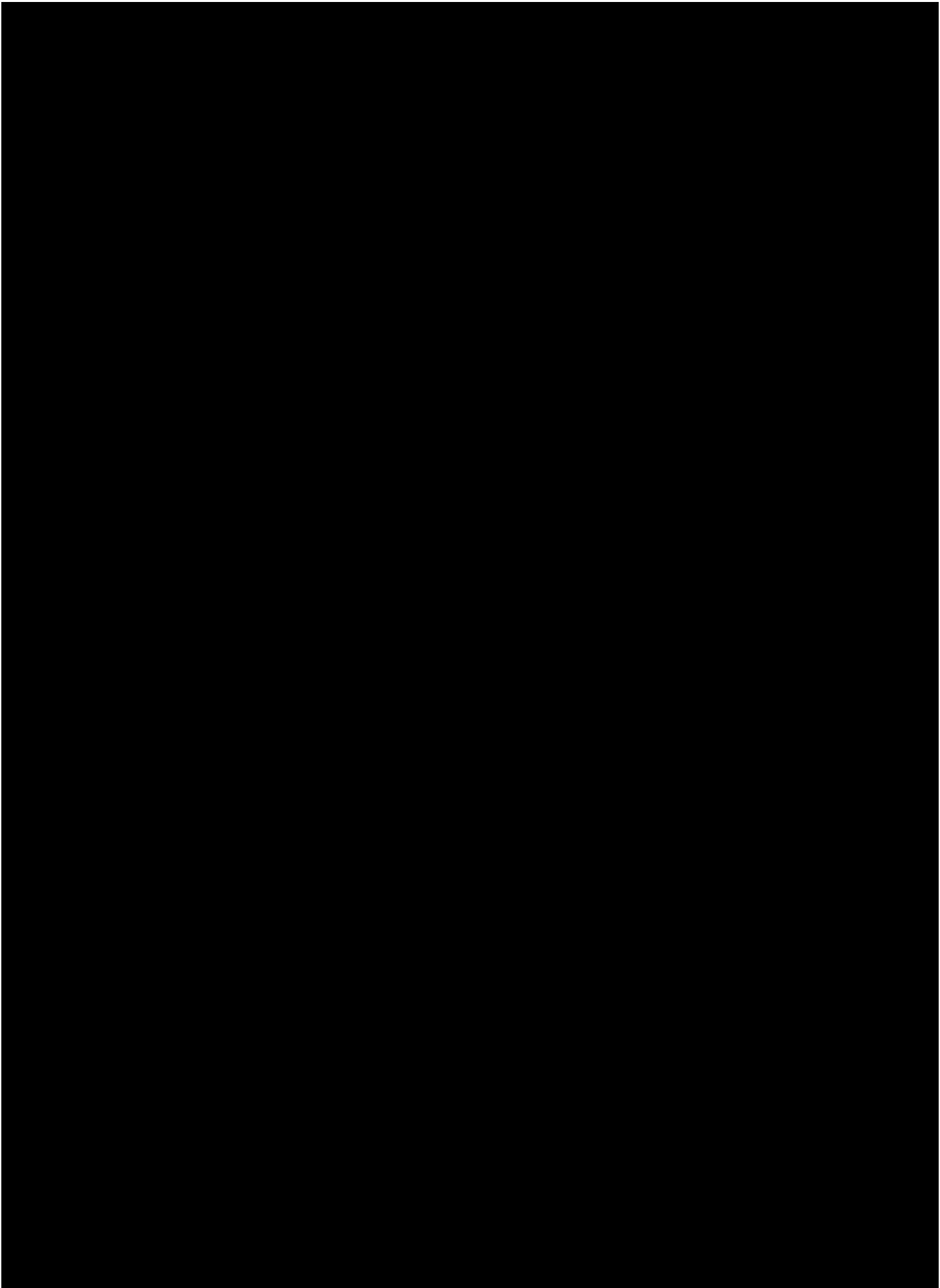
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



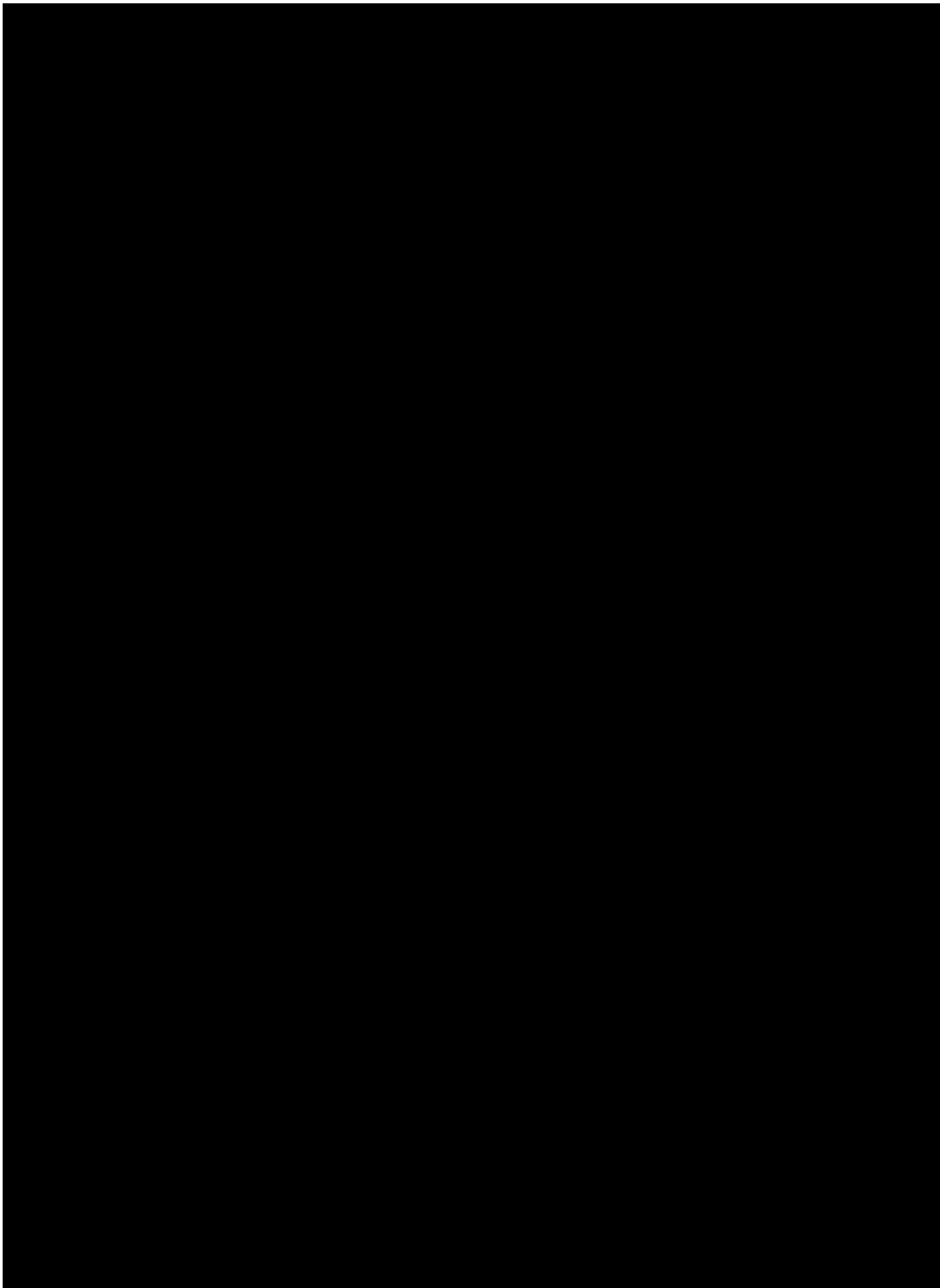
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

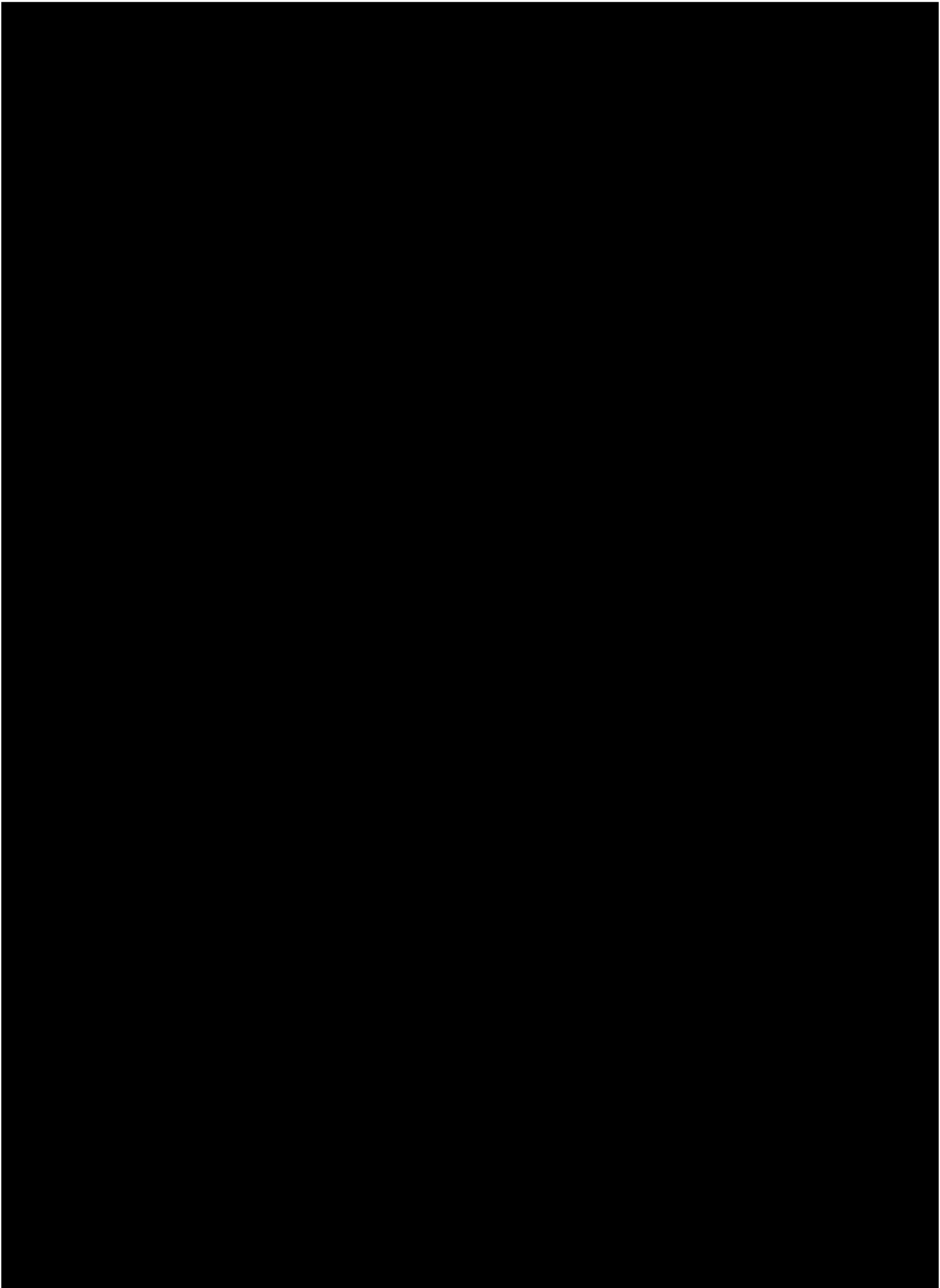
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

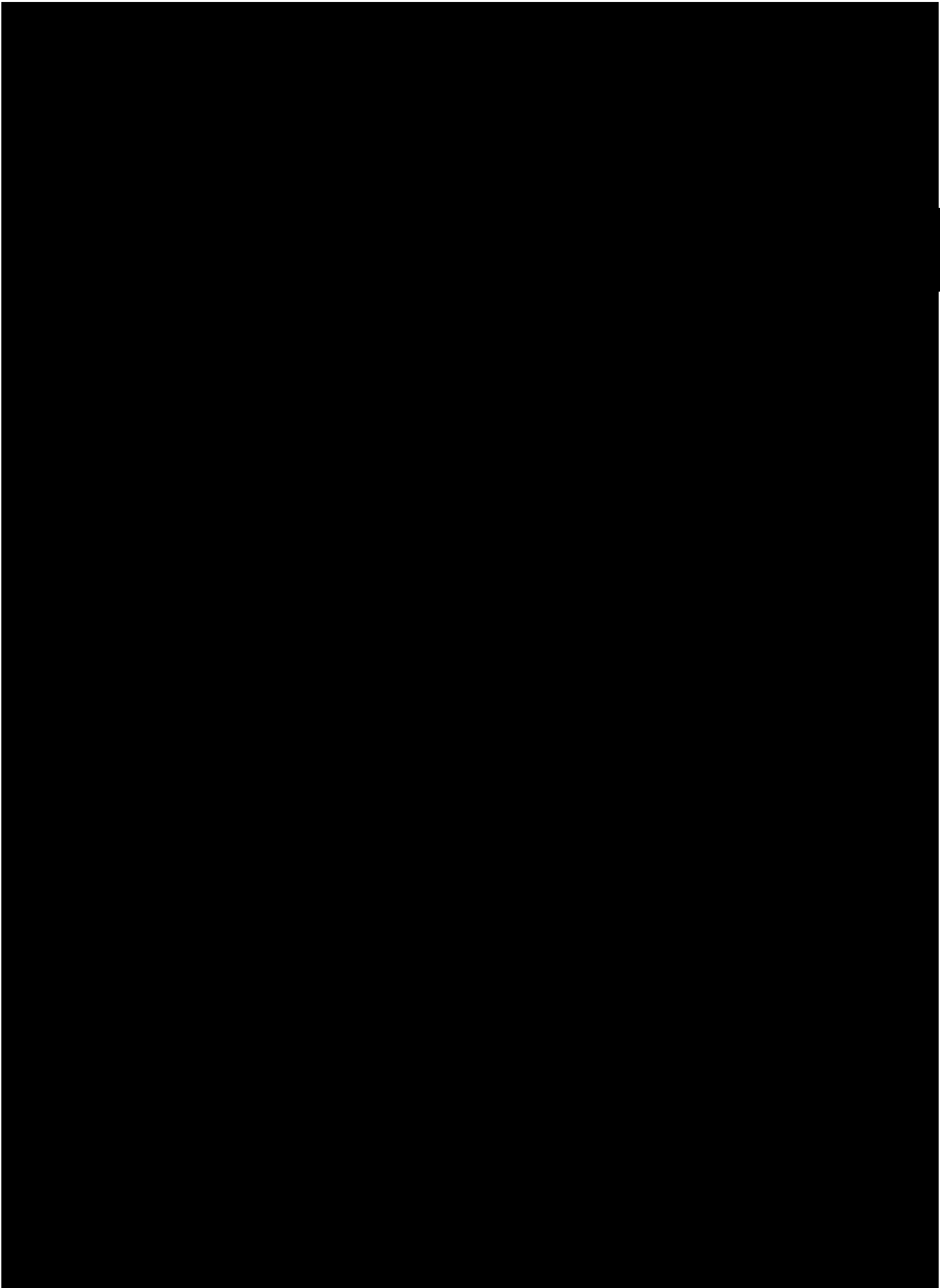
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

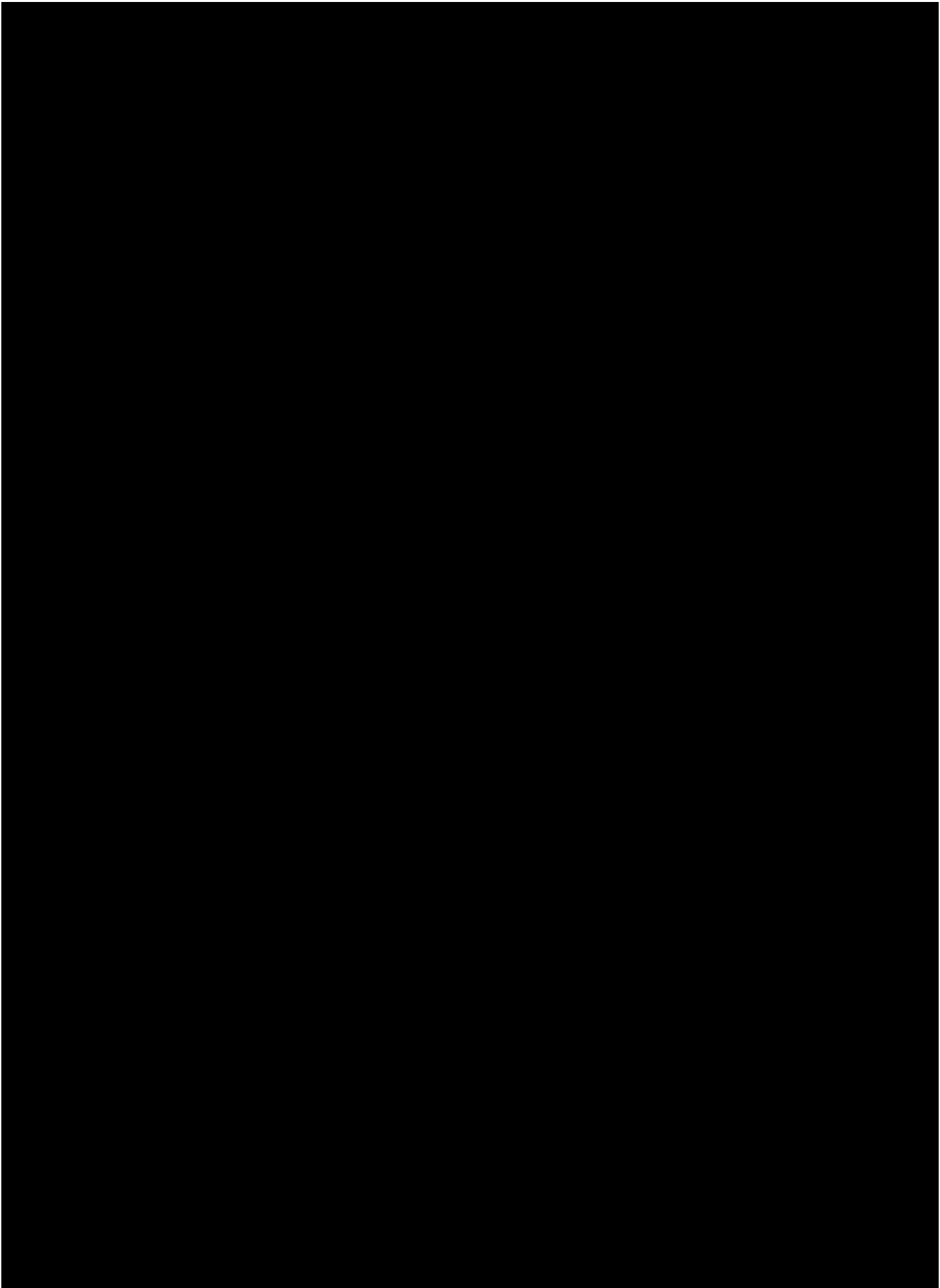
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

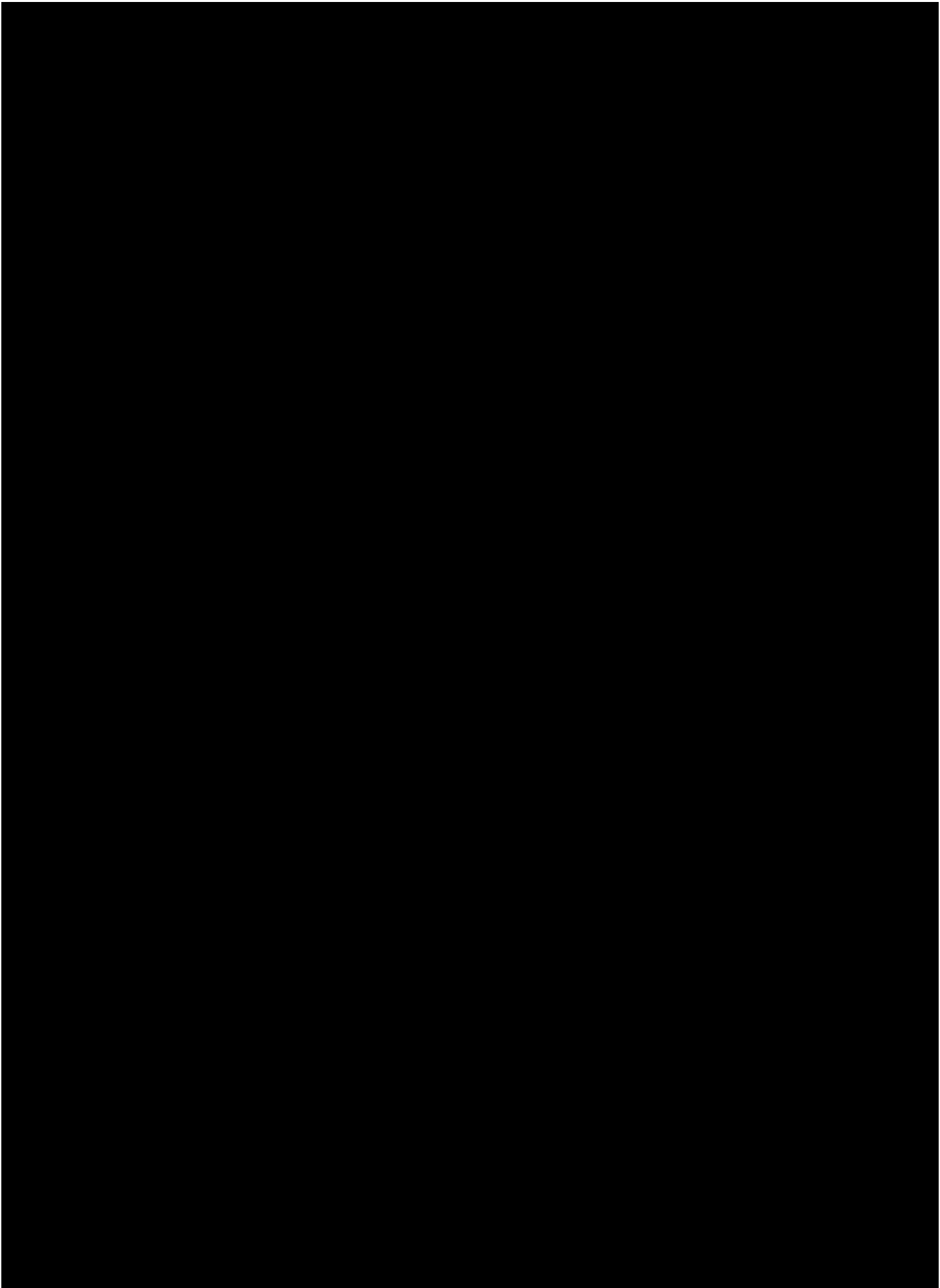
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



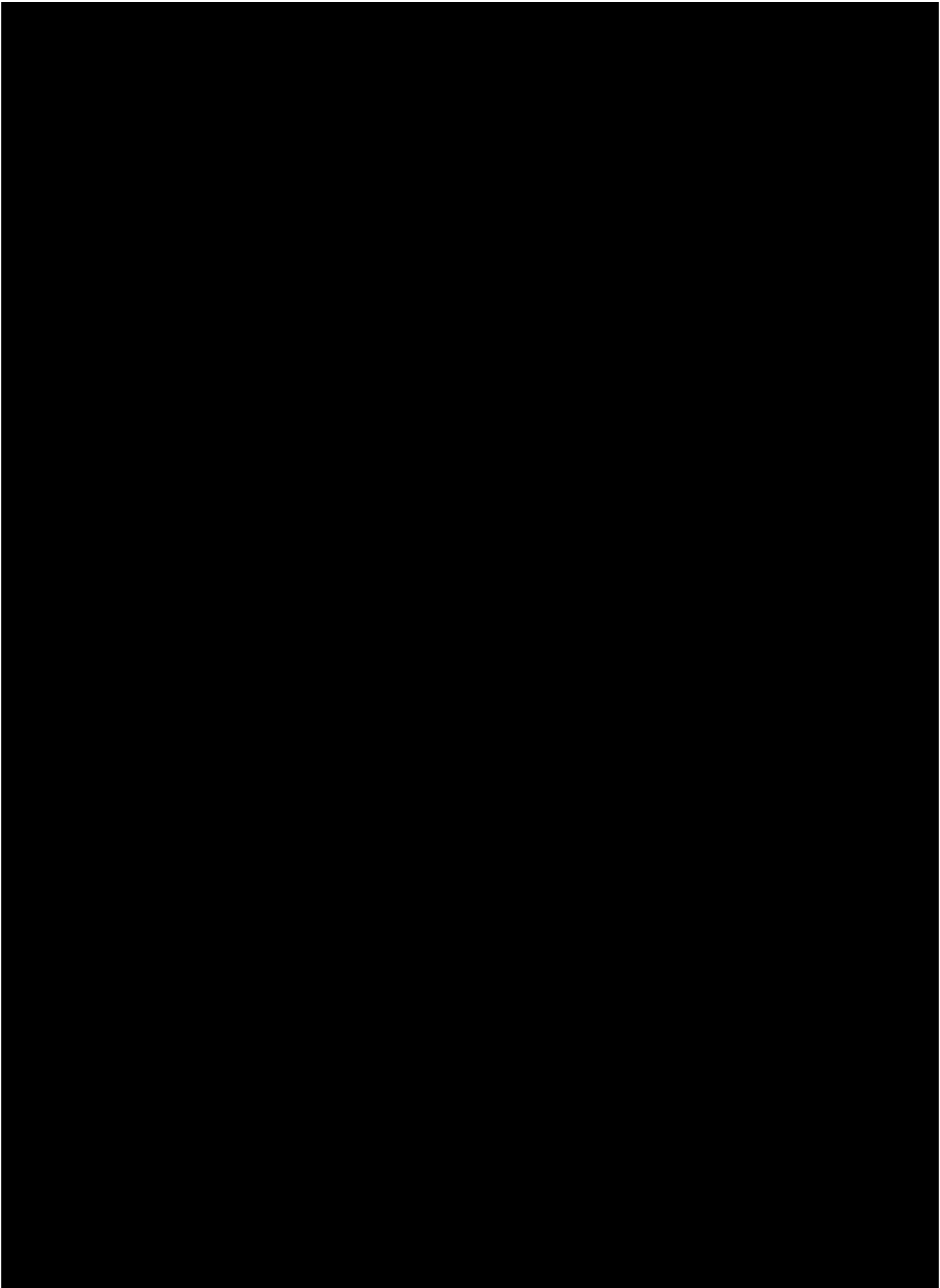
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]



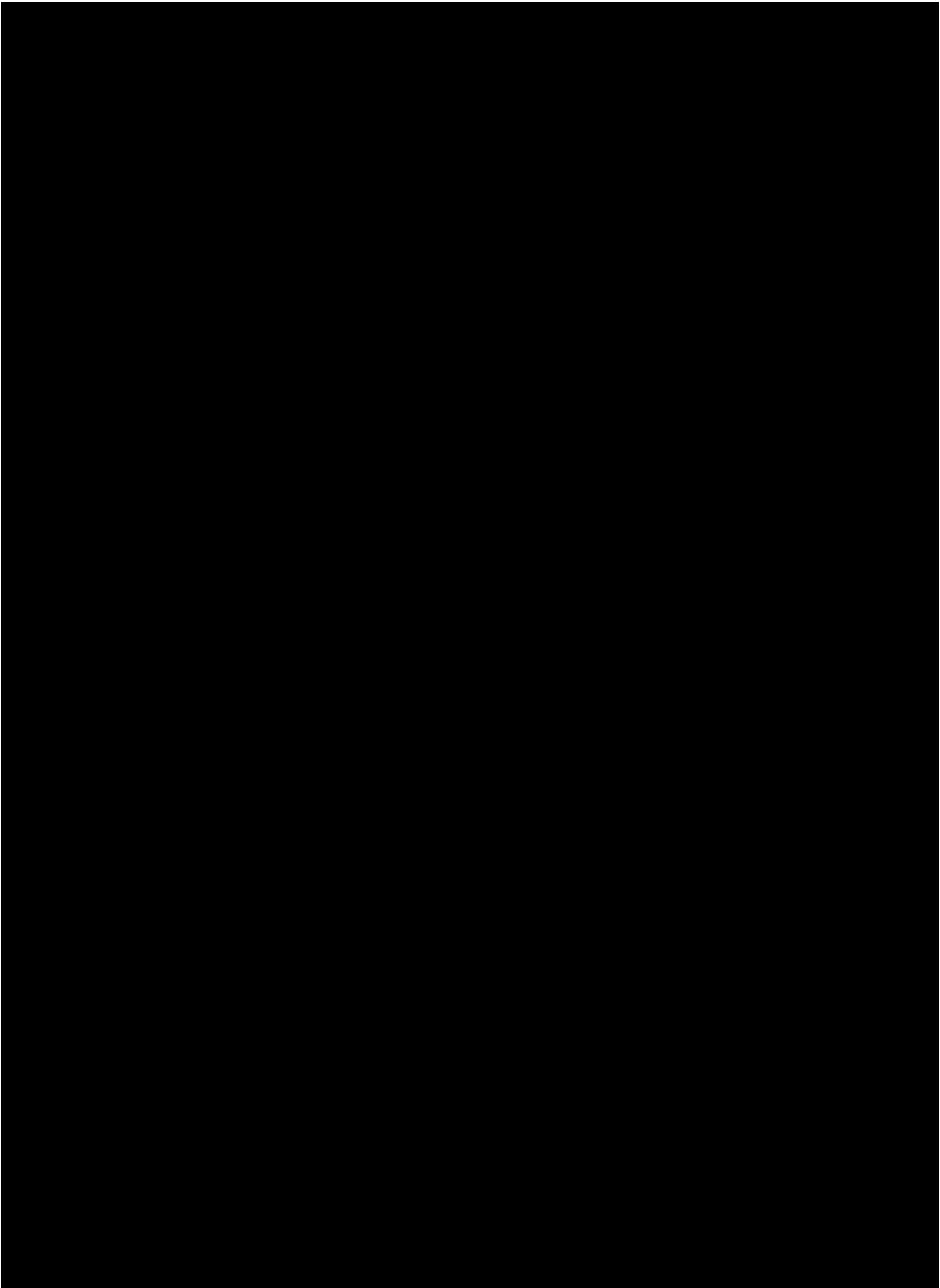
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]



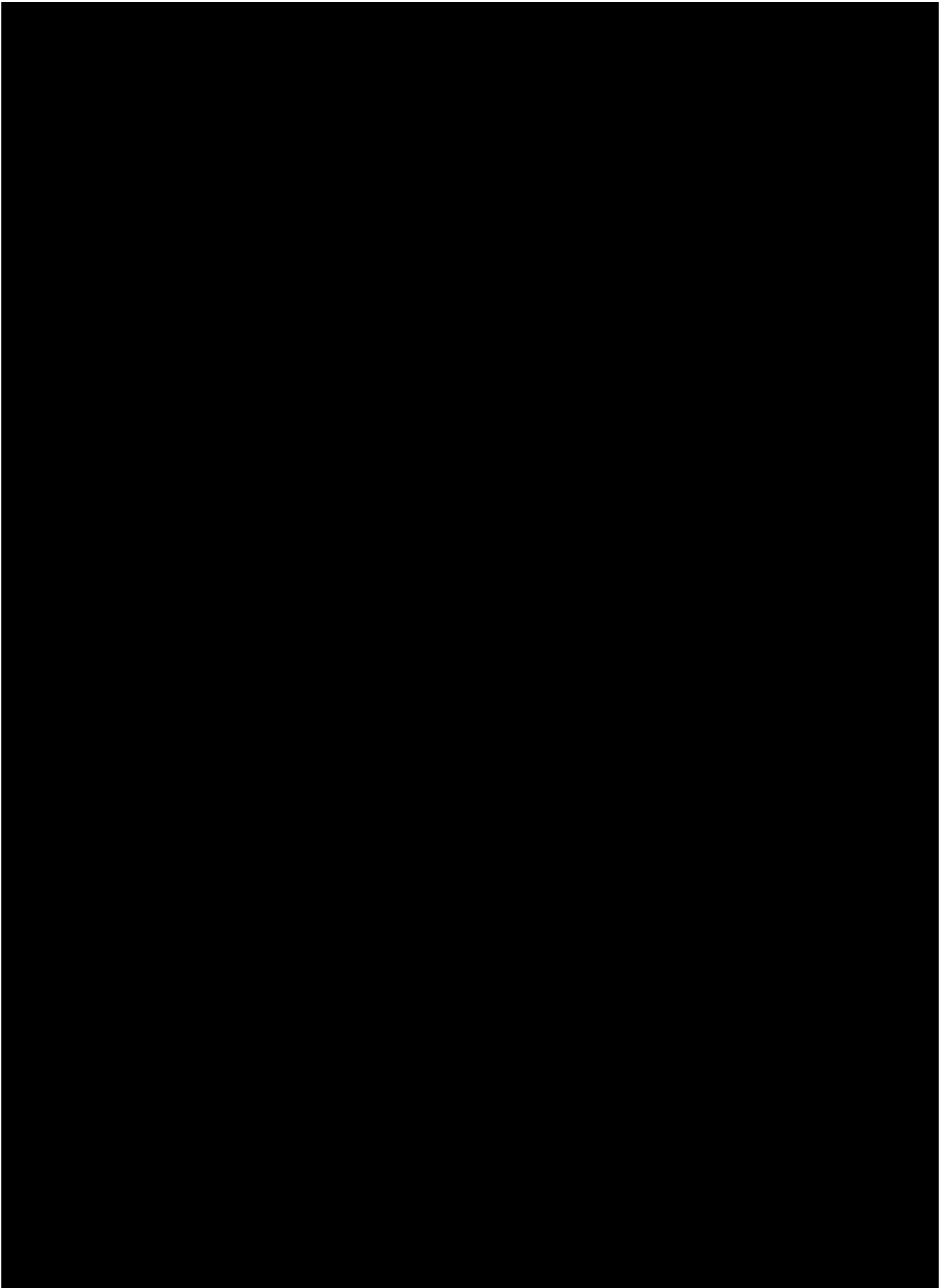
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]



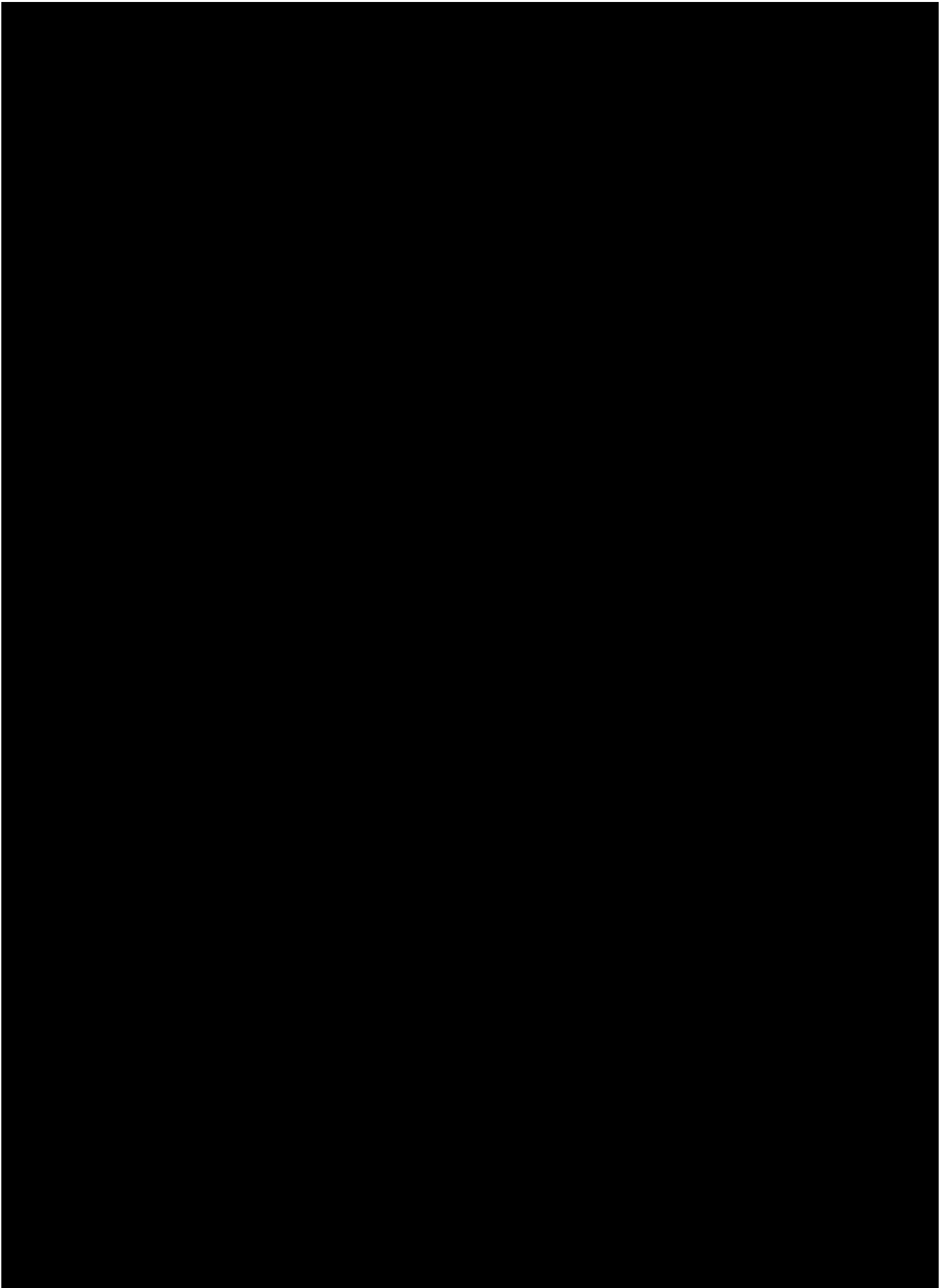
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

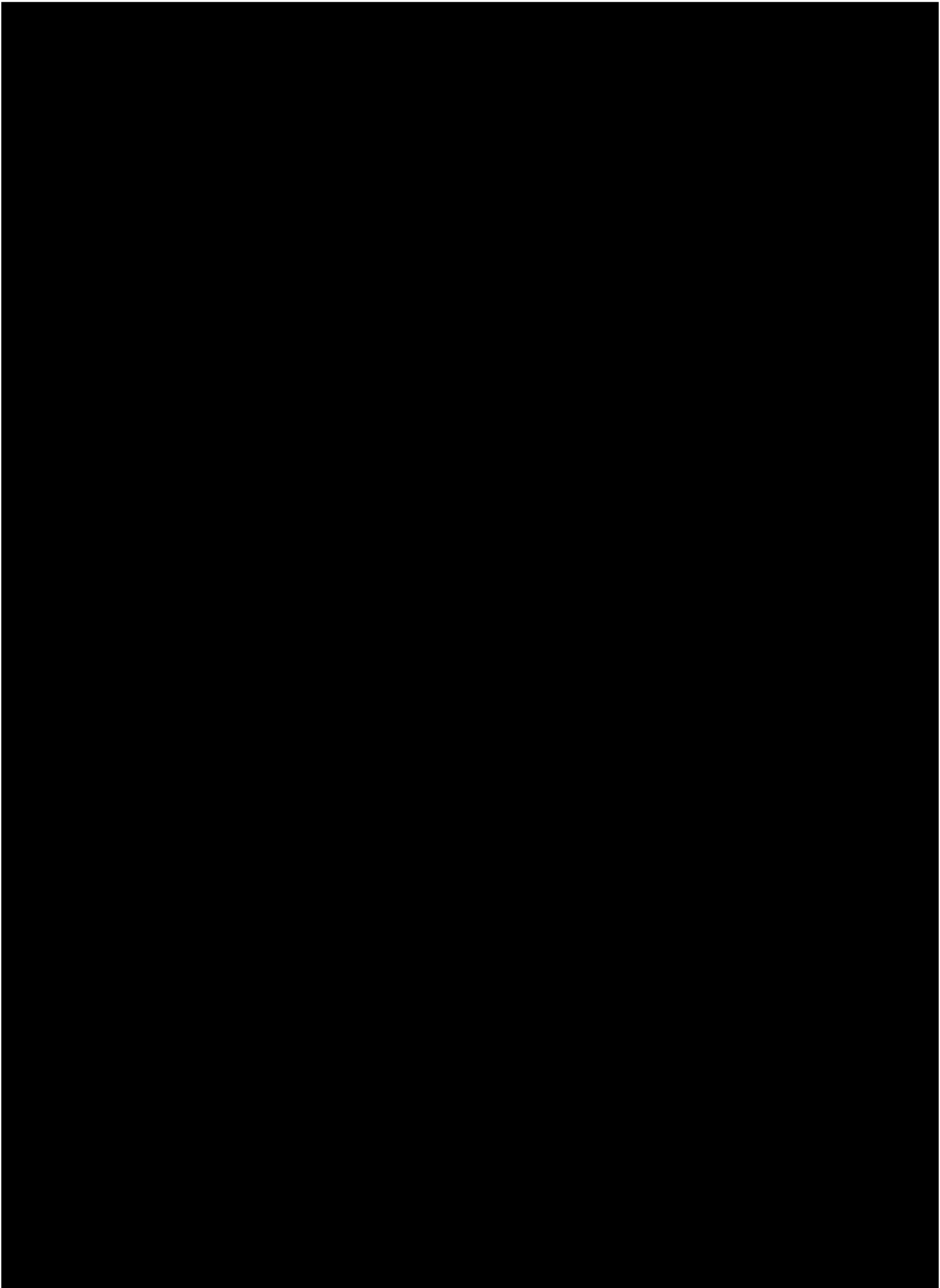
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



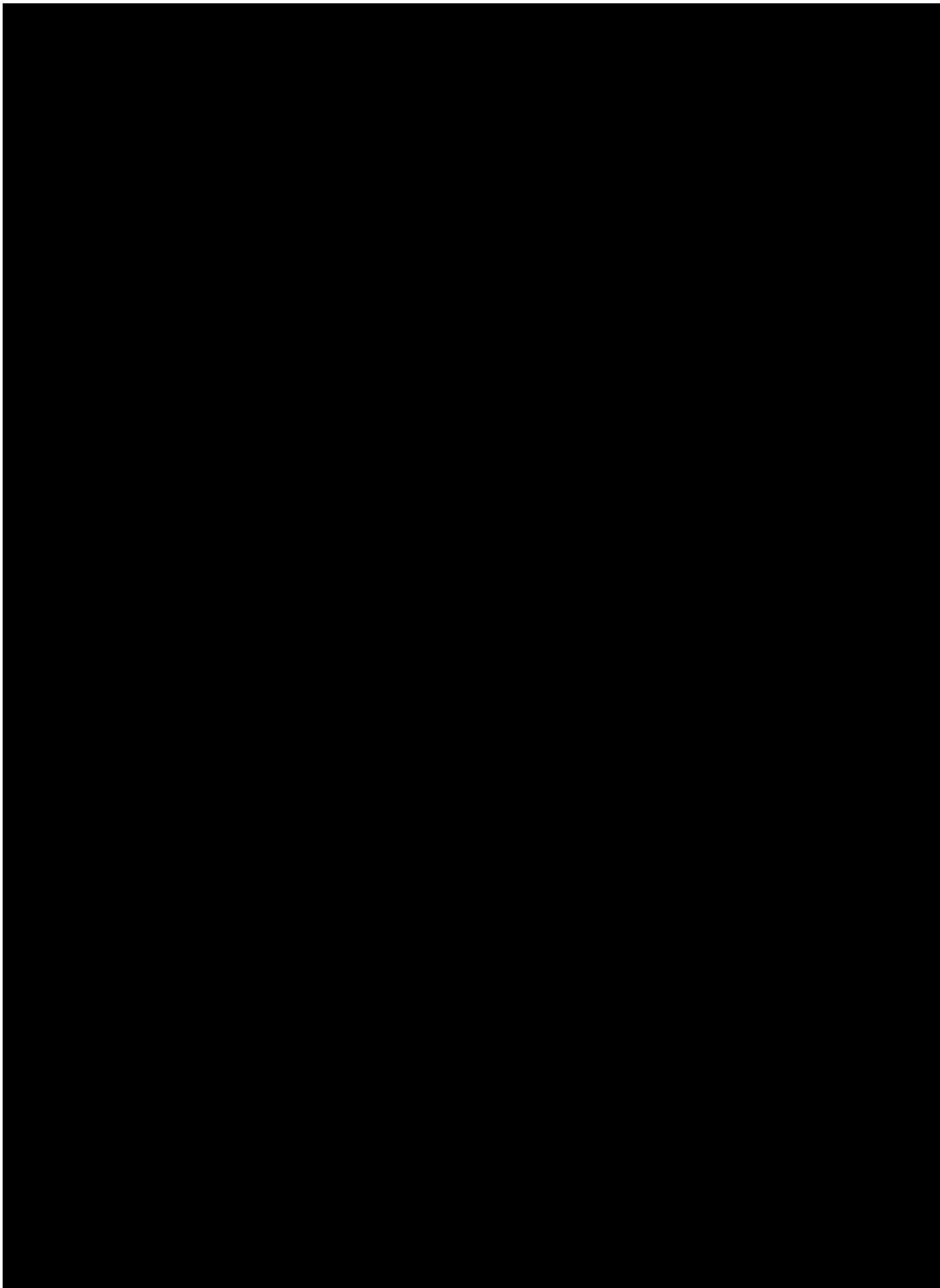
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]



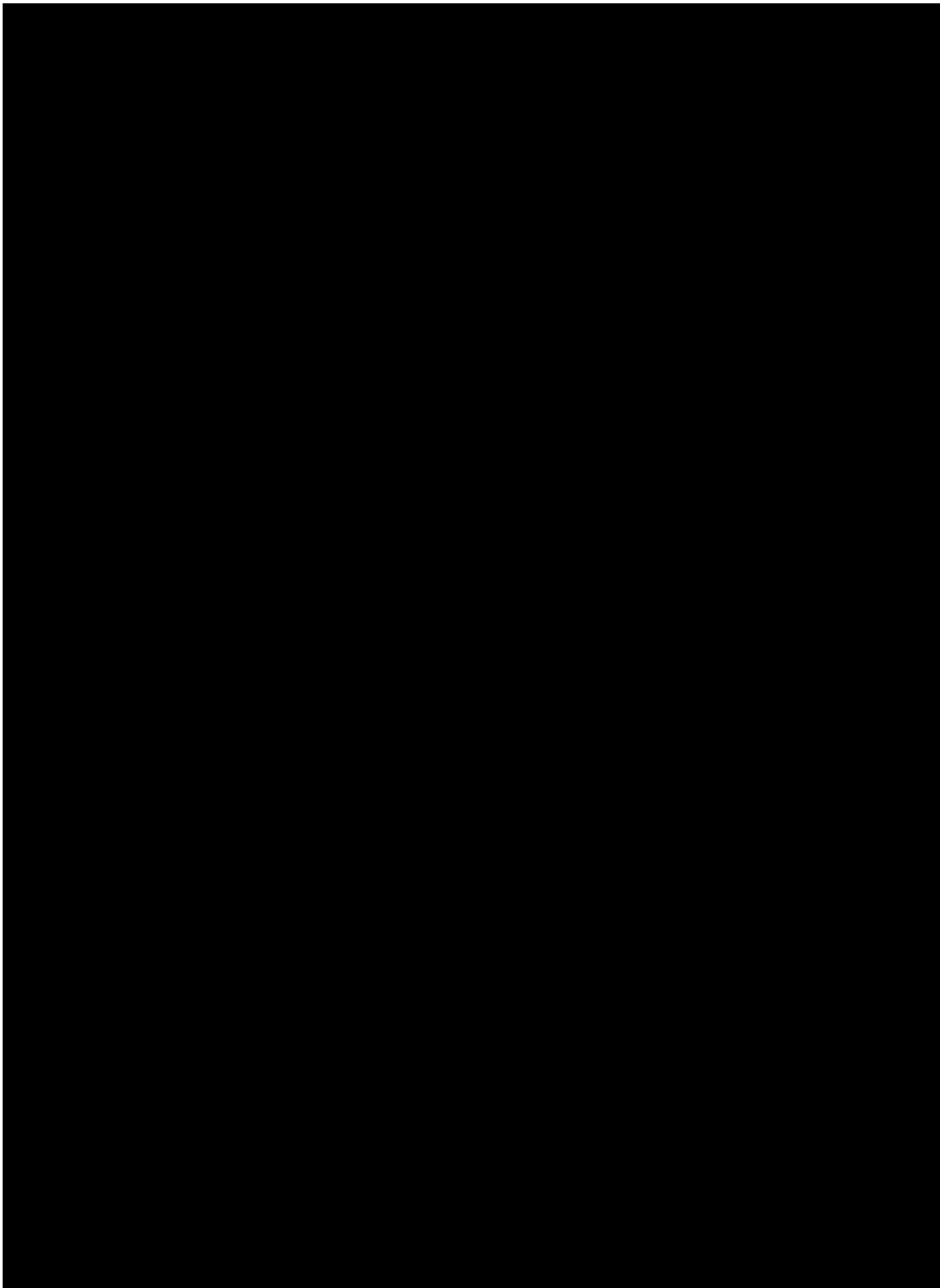
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

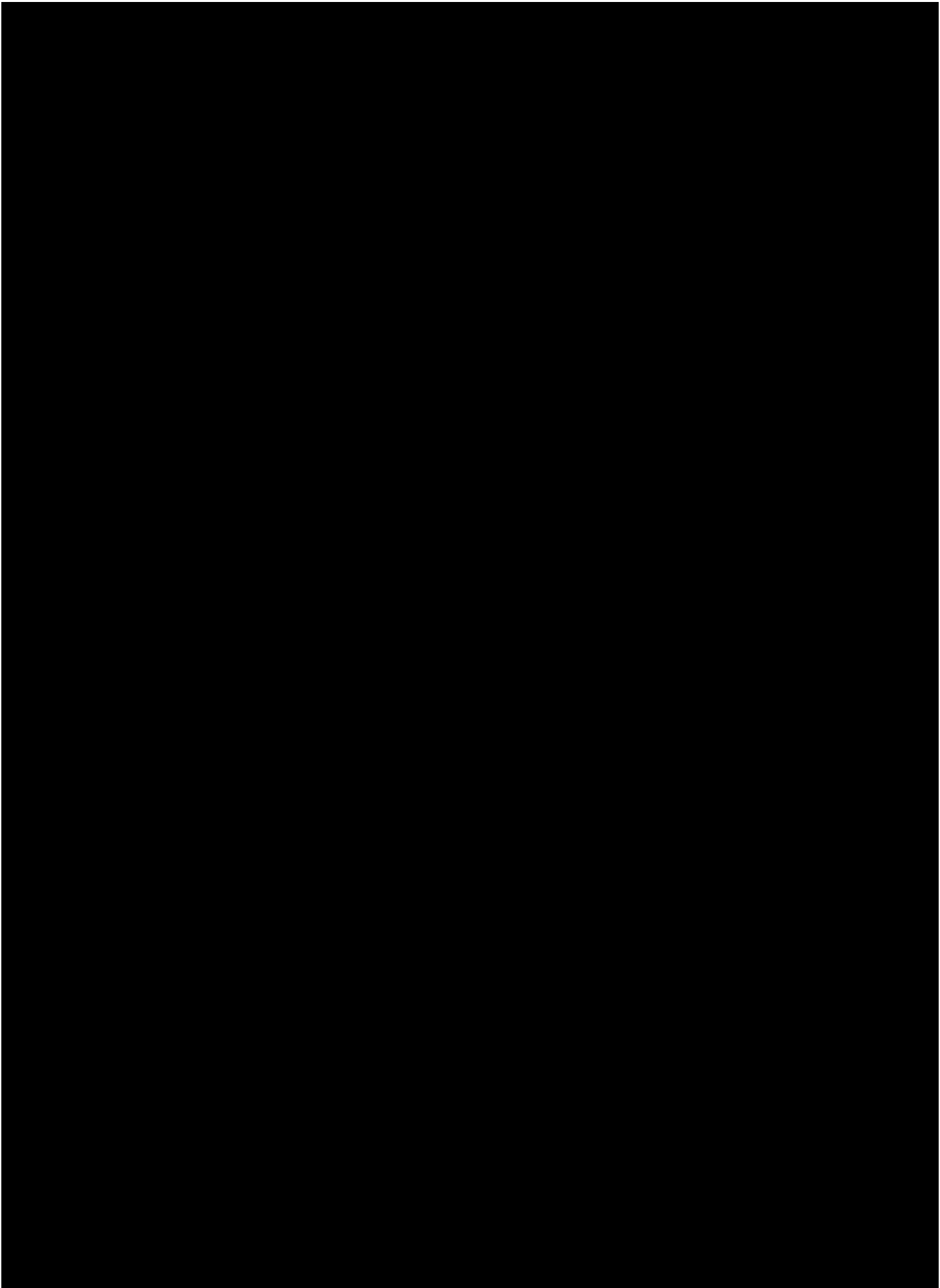
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

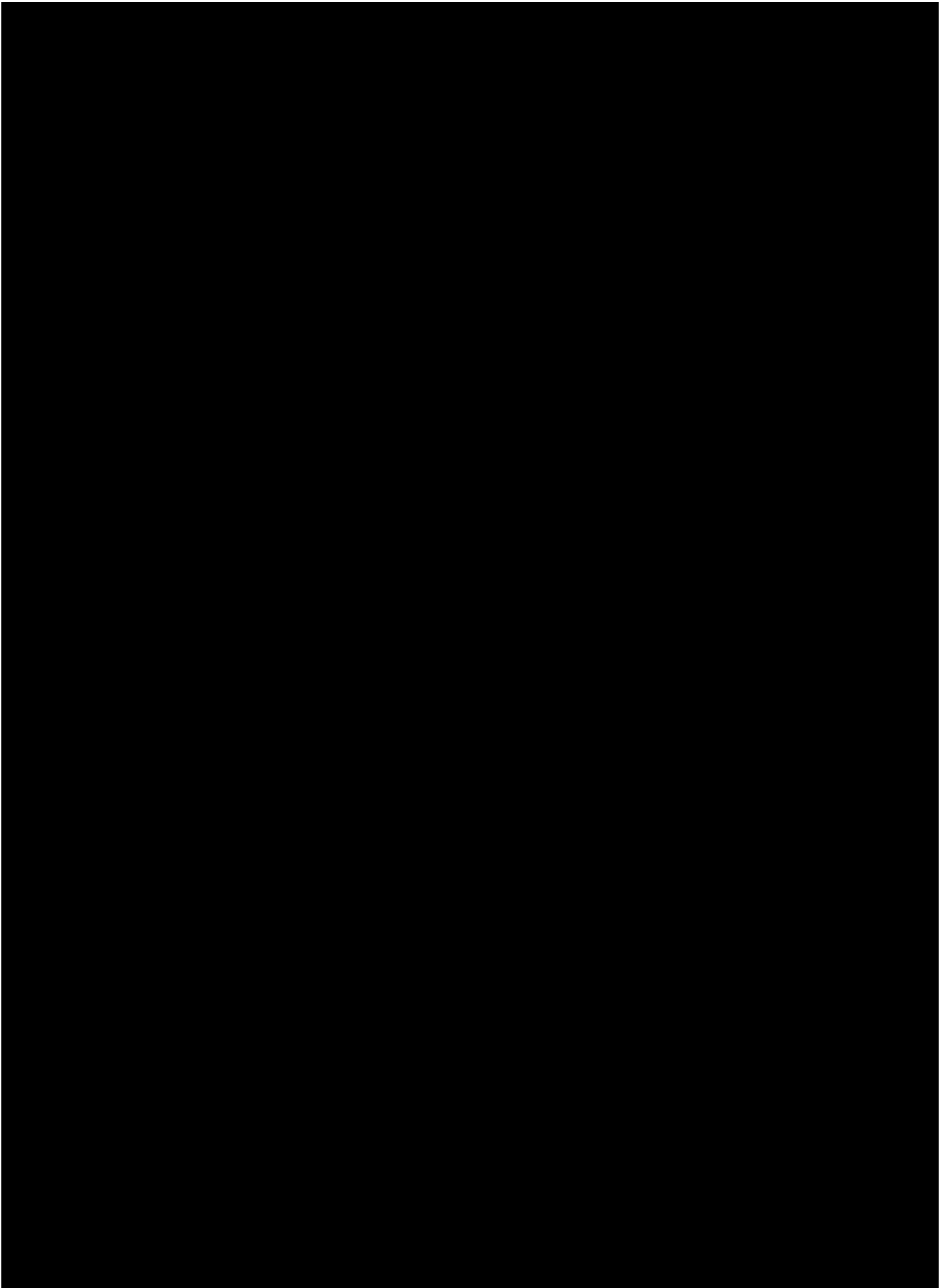
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

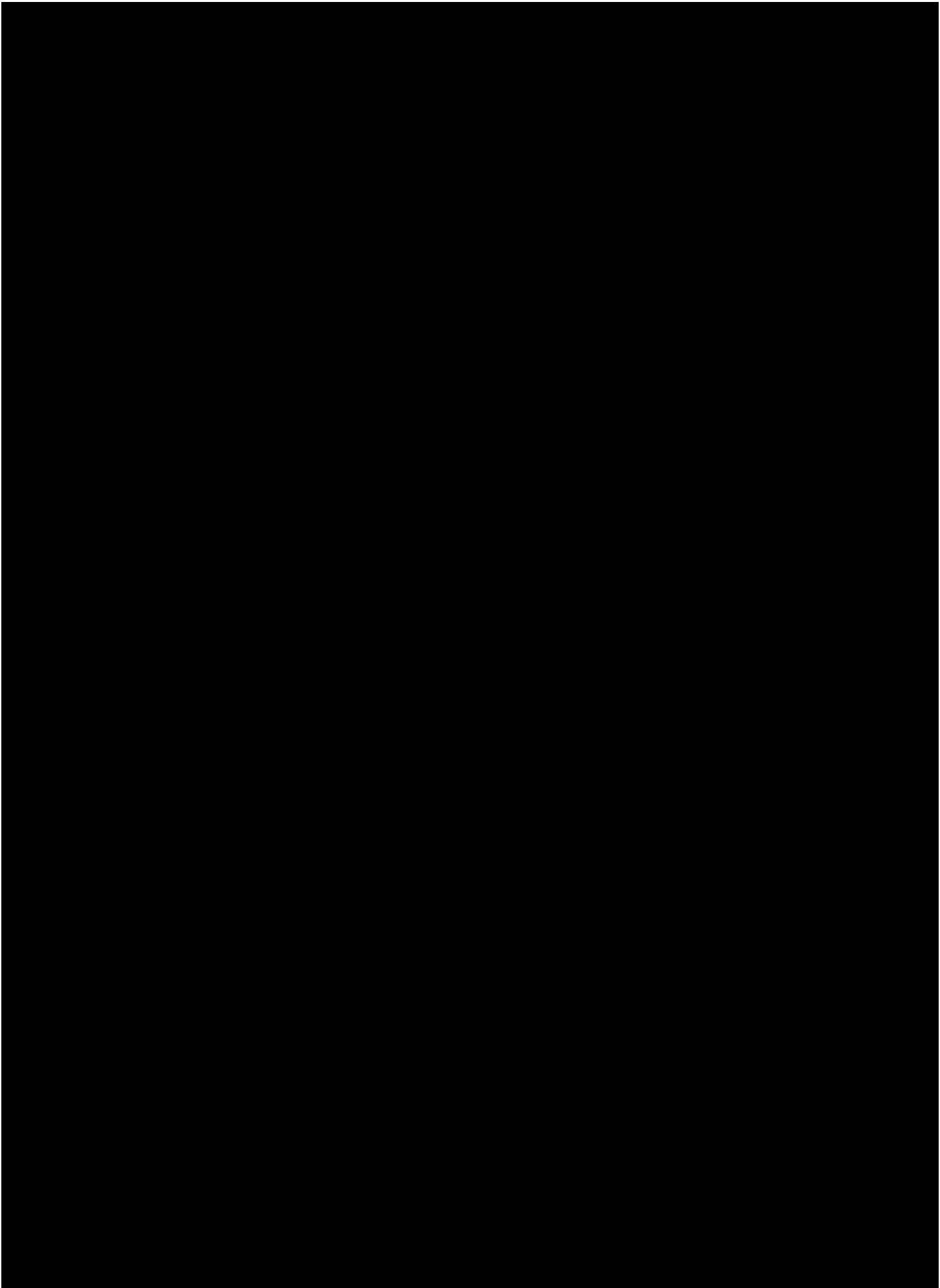
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

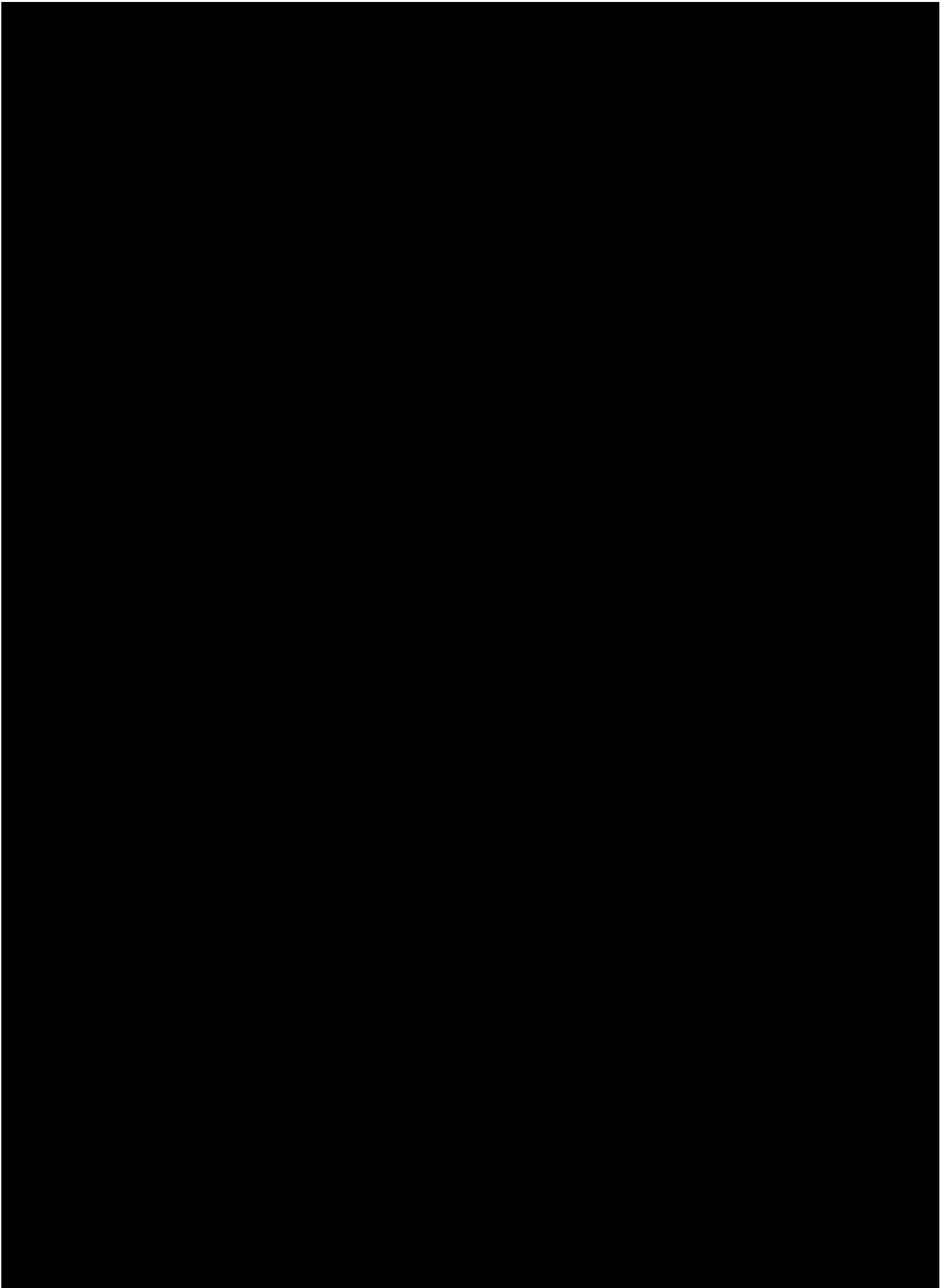
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



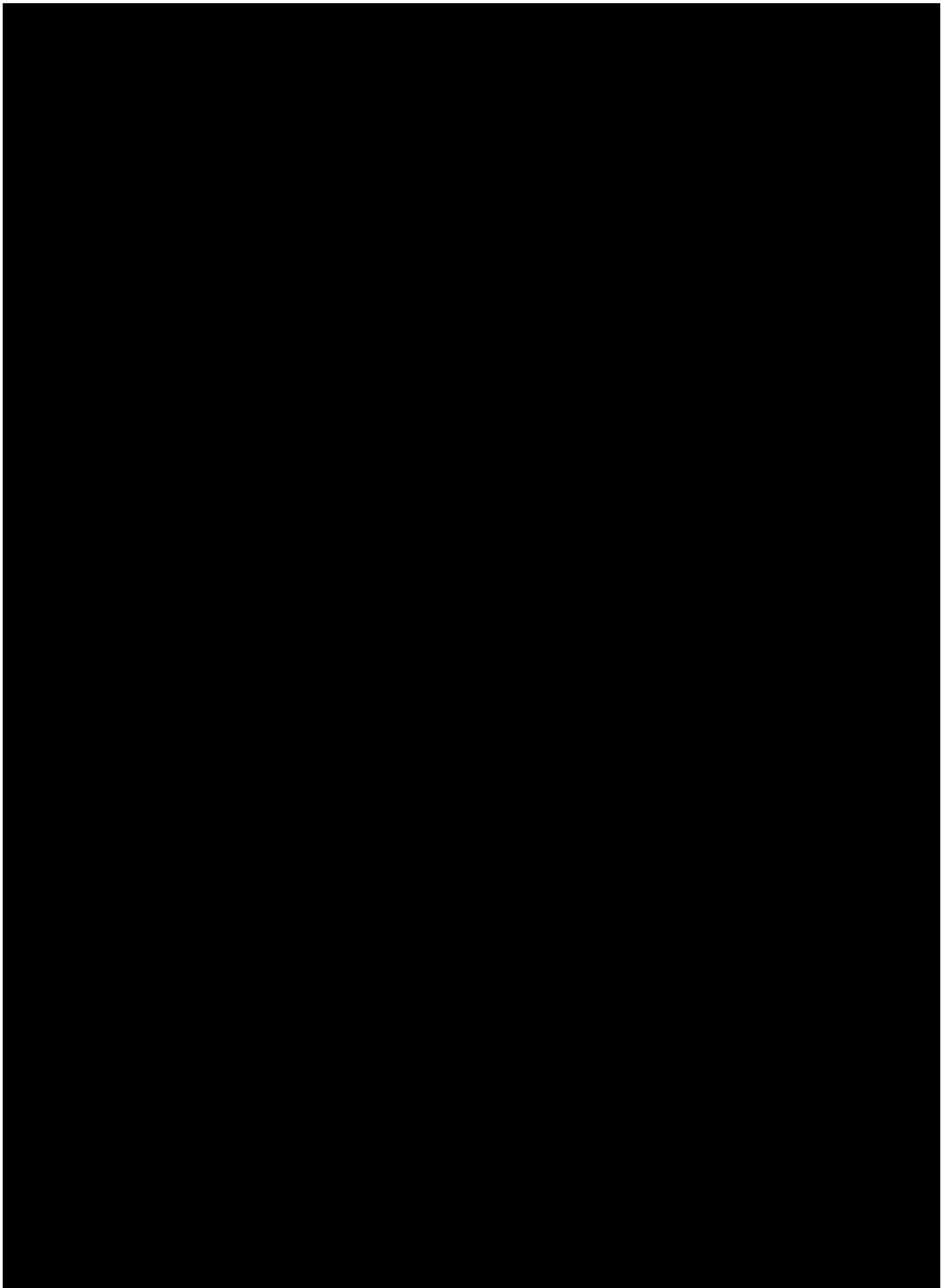
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]



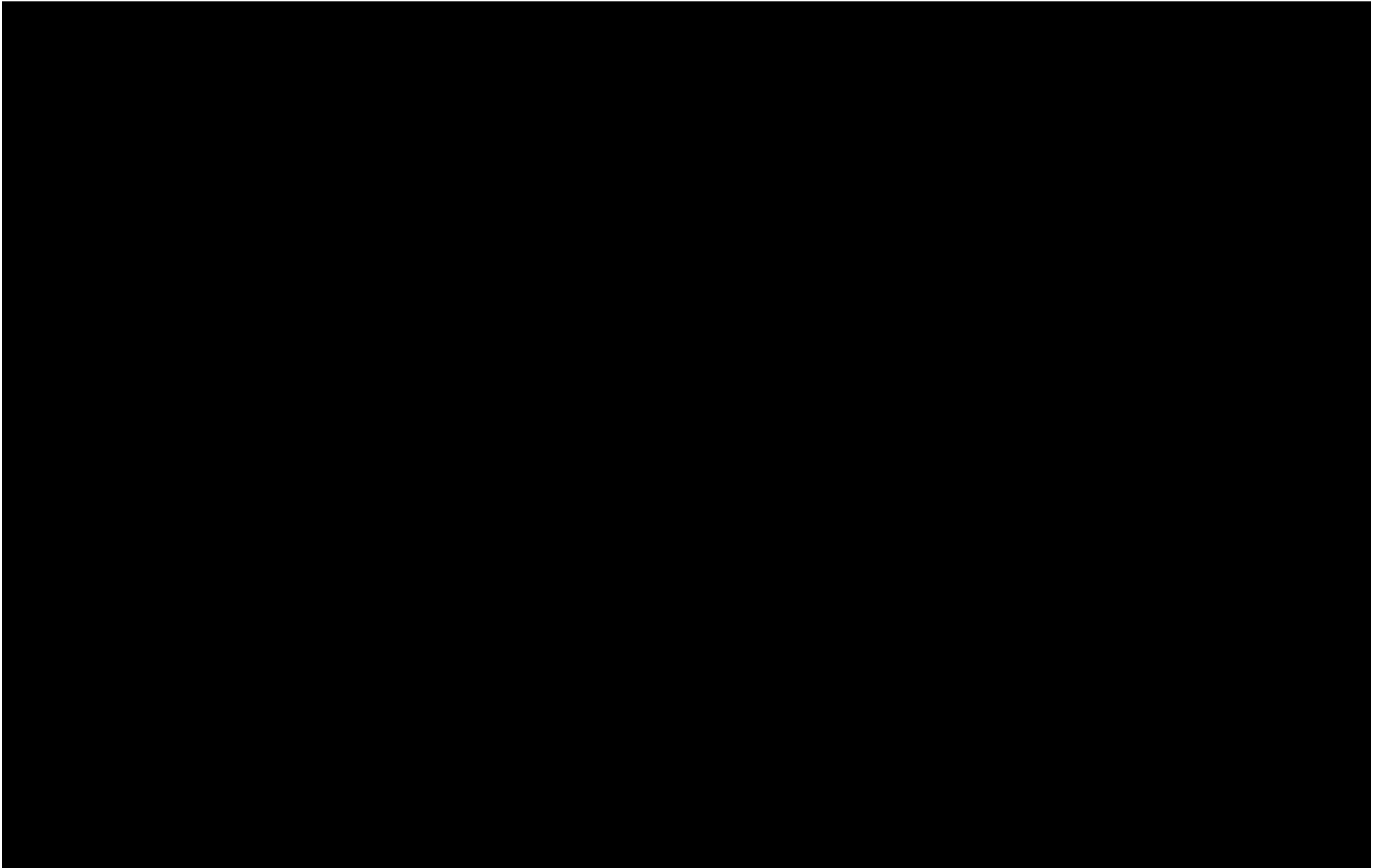
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]



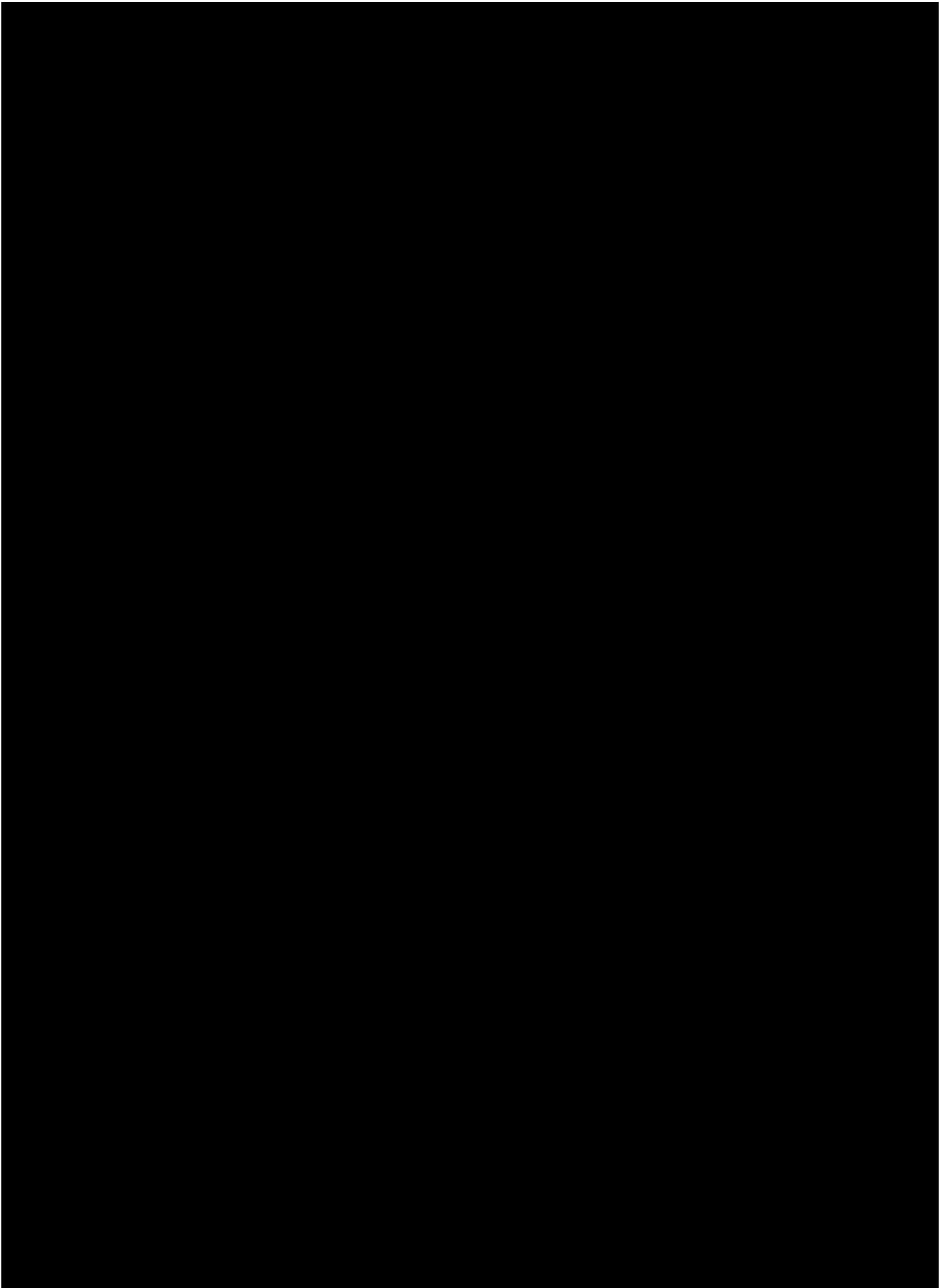
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

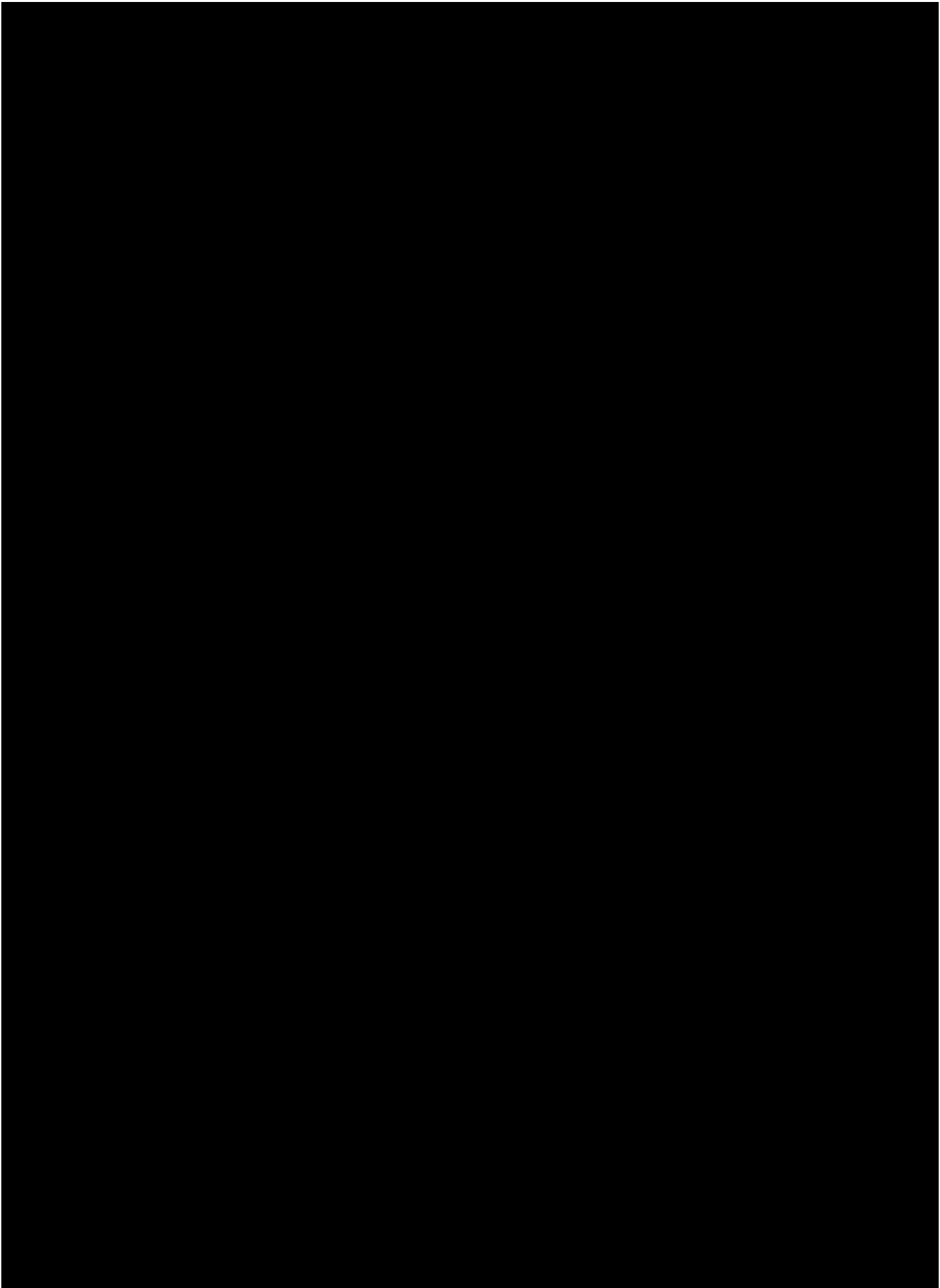
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

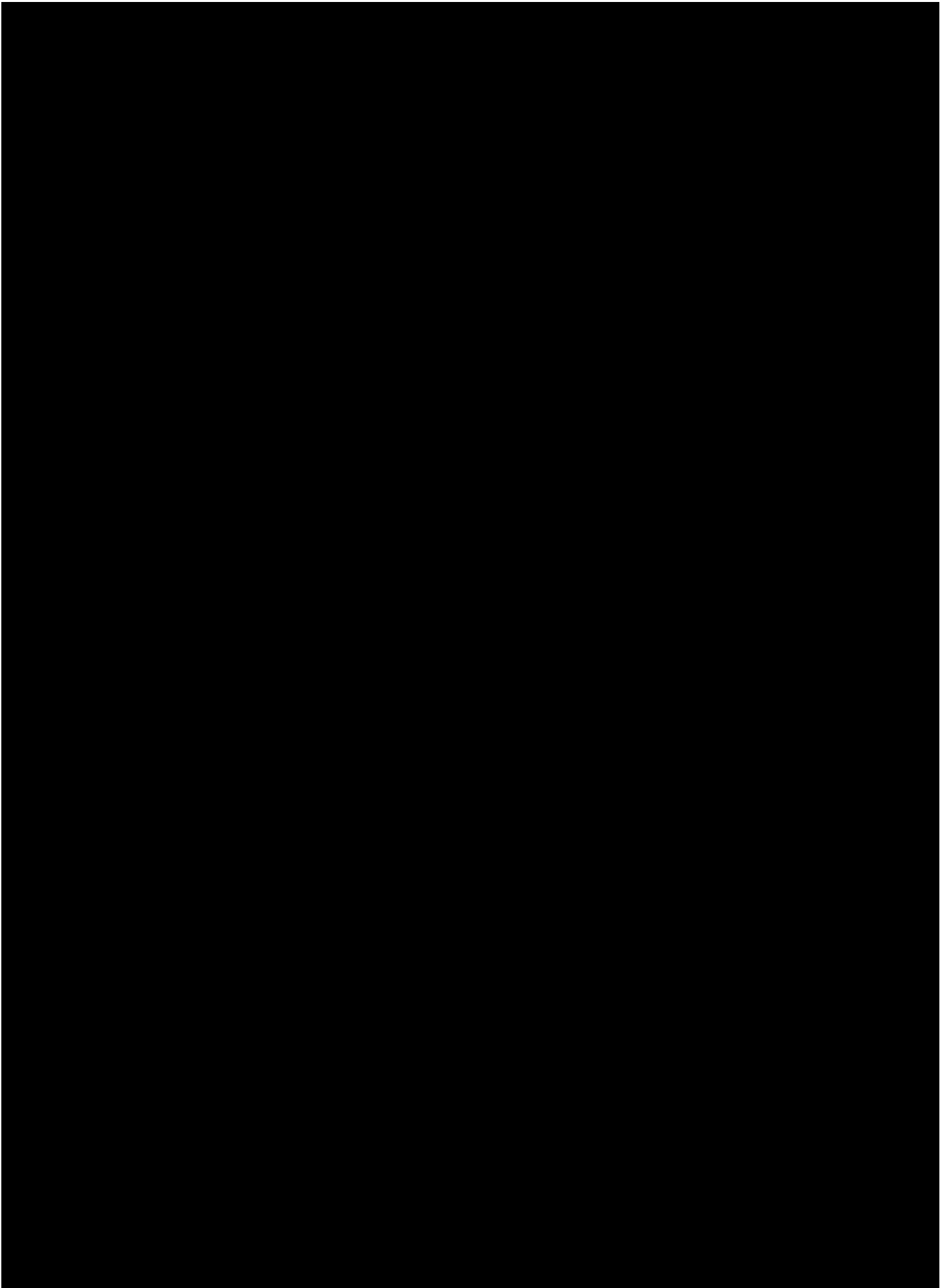
Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



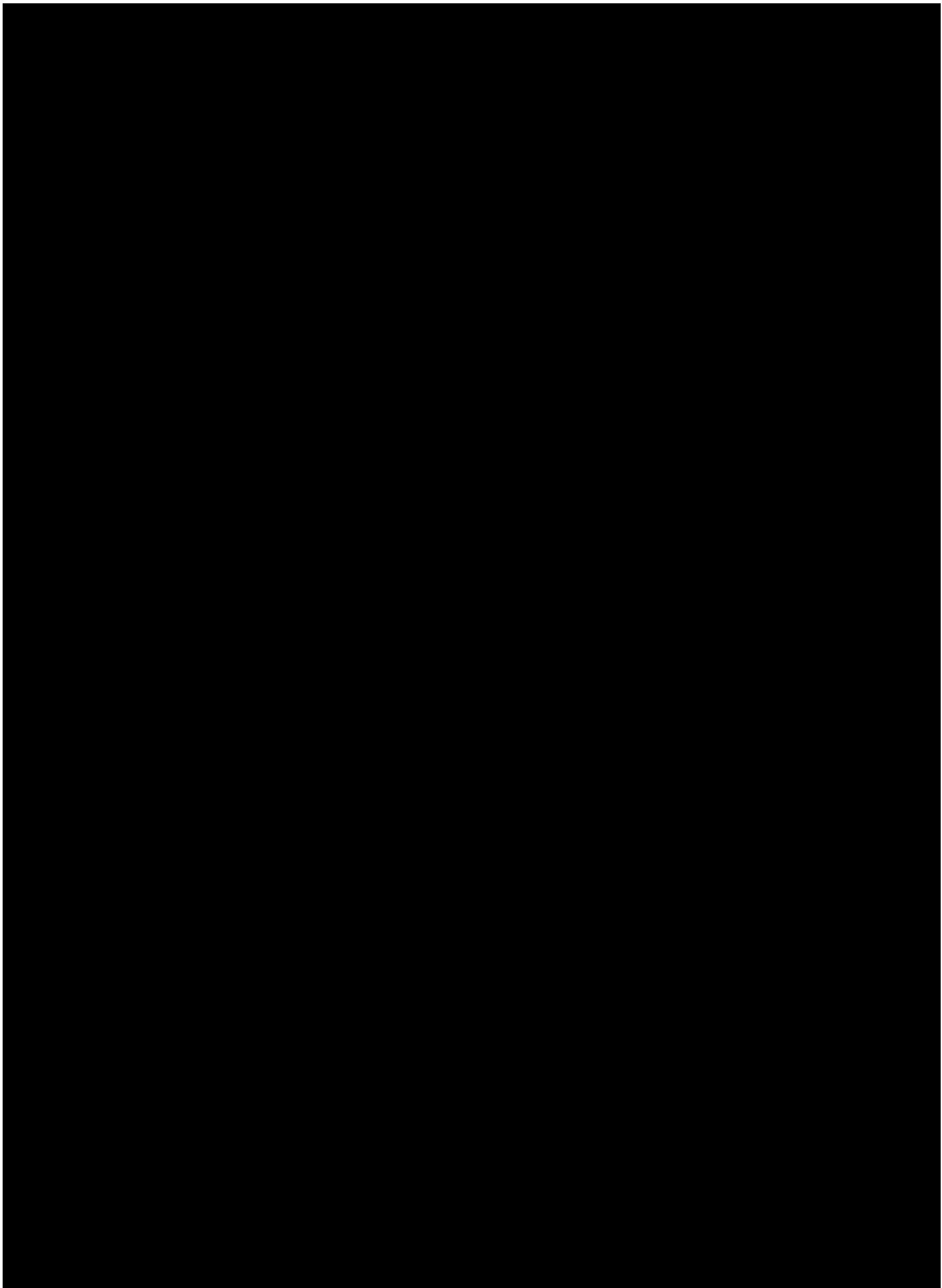
ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

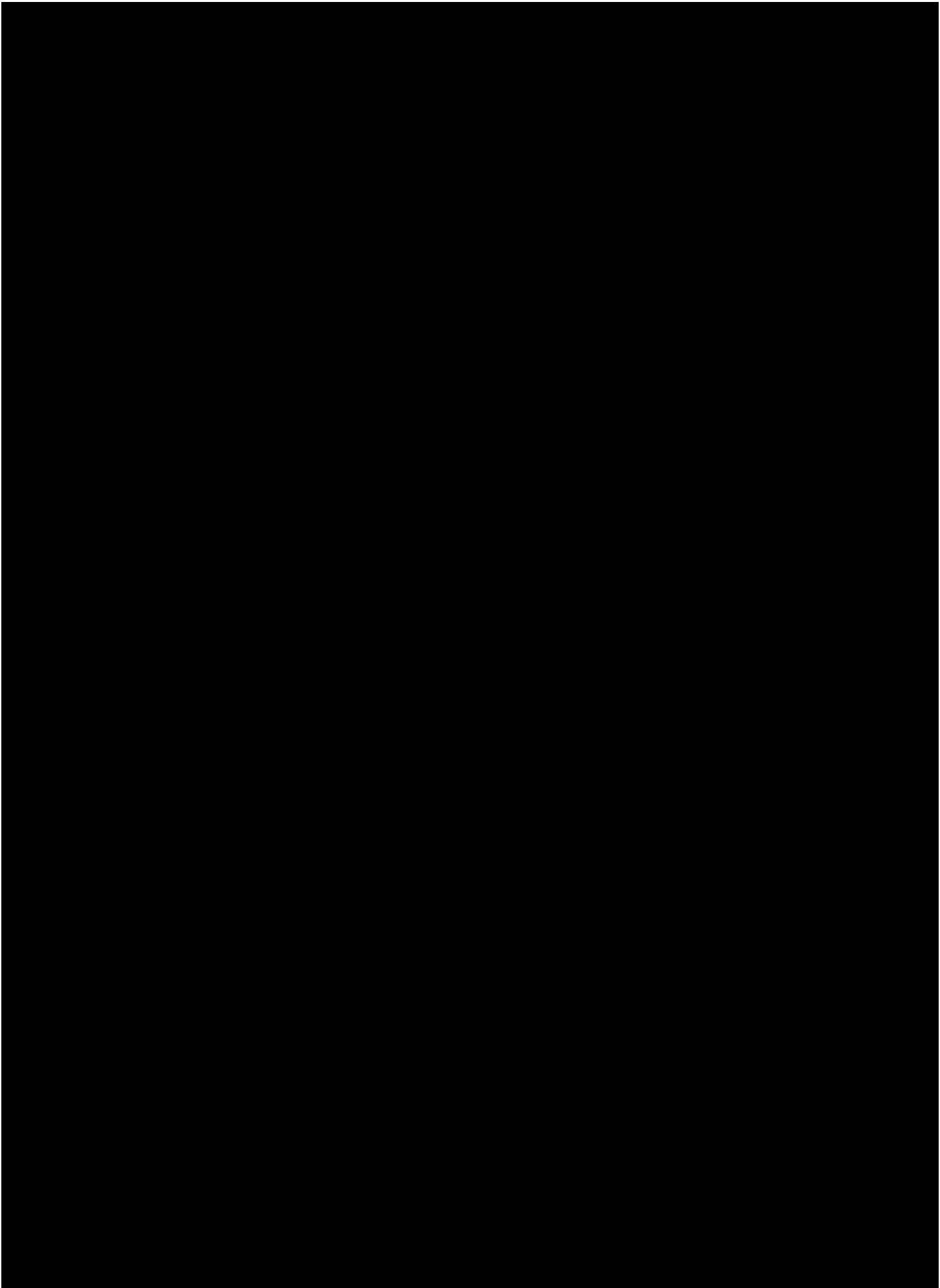
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]



ANNEX 8 (SUPPLIER TS SOLUTION) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

**ANNEX 9 (TS COMMERCIALY SENSITIVE INFORMATION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 9

TS COMMERCIALY SENSITIVE INFORMATION

**ANNEX 9 (TS COMMERCIALLY SENSITIVE INFORMATION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Annex 9 (*TS Commercially Sensitive Information*)

- 1 In this Annex the Parties have sought to identify the Supplier's Confidential Information in connection with the Transitional Services that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs (the “**TS Commercially Sensitive Information**”).
- 2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Annex 9 applies in the table below (please see the column “Duration of Confidentiality”).
- 3 Without prejudice to the Authority’s obligation to disclose Information in accordance with FOIA or Clause 19 (Confidentiality), and in addition to the information set out in Schedule 9 of this Contract, the Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following TS Commercially Sensitive Information:

TS Commercially Sensitive Information

No.	Item(s)	Duration of Confidentiality
1	TS Charges including, rate cards and any volume and utilisation discounts provided.	TS Term plus 6 years
2	Breakdown of pricing information to give input costs, capital and operating costs, overheads, revenue, margins and profits for the Transitional Services.	TS Term plus 6 years
3	How any payments due to the Supplier under this Schedule 34 on termination of the whole or any part of the Transitional Services have been or will be calculated but excluding the actual amounts of such payments.	TS Term plus 6 years
4	Any financial data relating to the Supplier’s business as a whole including the financial standing of the Supplier provided in connection with this Schedule 34, including but not limited to any information relating to Financial Distress reporting.	TS Term plus 6 years

**ANNEX 9 (TS COMMERCIALLY SENSITIVE INFORMATION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

No.	Item(s)	Duration of Confidentiality
5	Liability and Indemnities in this Schedule 34; including the amount of any caps, any unlimited heads of losses and any excluded heads of losses.	TS Term plus 6 years
6	The cover and amounts of the Supplier's Insurances.	TS Term plus 6 years
7	How any TS Service Credits are financially calculated under this Schedule 34, but excluding the details regarding the applicable service thresholds, or any performance related information or requirements, or information relating to the actual amounts of any TS Service Credits paid or credited to the Authority.	TS Term plus 6 years
8	Technical details of the Supplier's network (including topology, network diagrams, detailed network coverage, route maps, the Supplier's Points of Presence and/or street furniture/chambers etc.) for the Transitional Services.	TS Term plus 6 years
9	Design documents relating to the Transitional Services prepared or delivered by the Supplier and any notes or minutes of technical design meetings held in relation to the aforementioned but excluding any documents set out in this Contract as being TS Deliverables to the Authority.	TS Term plus 6 years
10	Any Supplier proposals in response to TS Change Requests to the extent that the information falls within one of the other items set out in this table and innovation proposals provided under this Schedule 34 relating to the Transitional Services (including in a response to a Change Request).	TS Term plus 6 years
11	Staff information generally including personal details and details of any TS Key Personnel.	TS Term plus 6 years
12	The Supplier's own Business Continuity Plan, Business Incident Plans, and Disaster Recovery Manuals and Procedures, Security Plan and Related Business Security Processes but excluding any Supplier or Authority specific plans or procedures to	TS Term plus 6 years

**ANNEX 9 (TS COMMERCIALLY SENSITIVE INFORMATION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

No.	Item(s)	Duration of Confidentiality
	be provided by the Supplier relating to the Transitional Services.	

**ANNEX 10 (NOTIFIED TS KEY SUB-CONTRACTORS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 10

NOTIFIED TS KEY SUB-CONTRACTORS

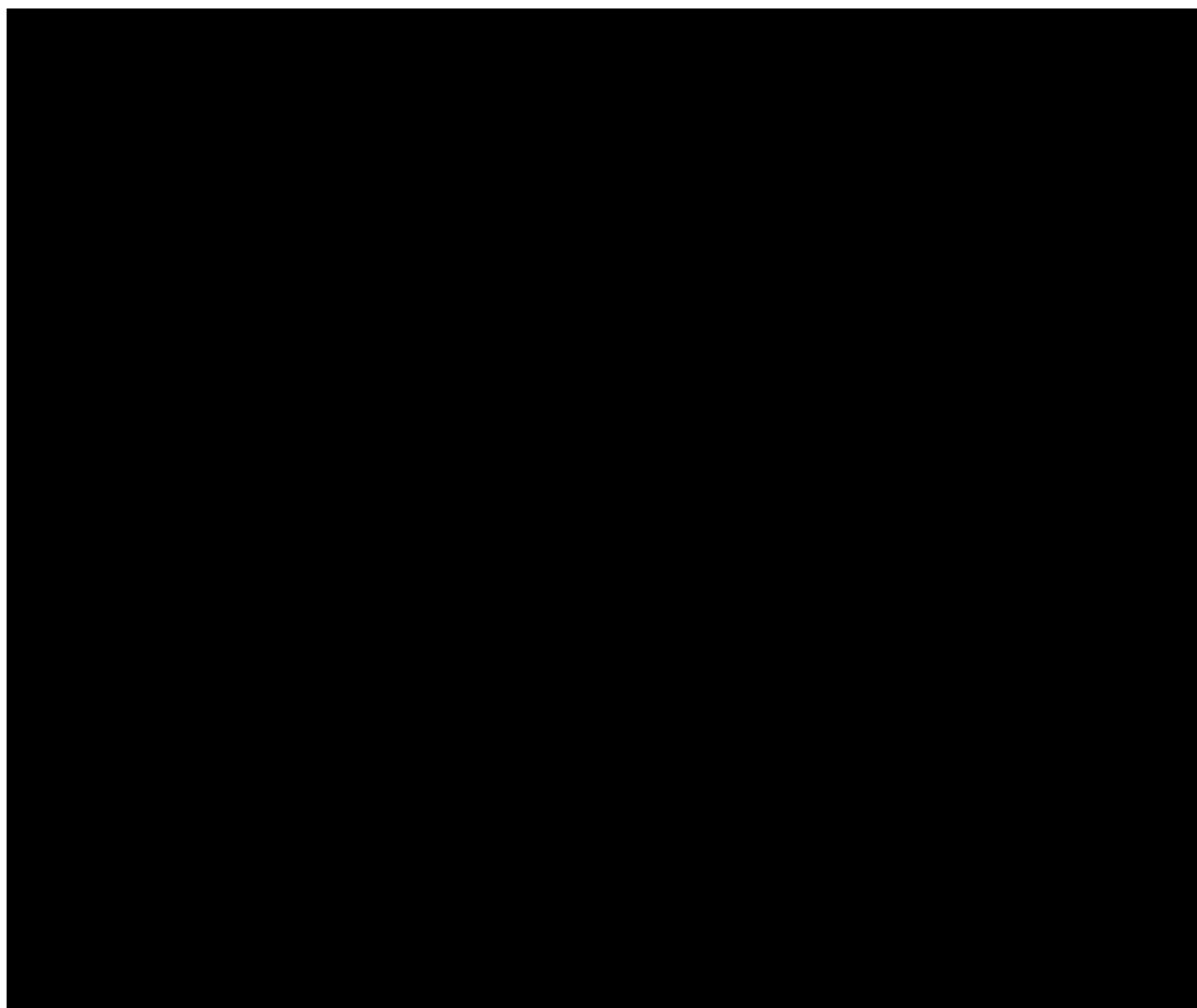
**ANNEX 10 (NOTIFIED TS KEY SUB-CONTRACTORS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Annex 10 (*Notified TS Key Sub-Contractors*)

- 1 In accordance with Paragraph 15.3 (*Appointment of TS Key Sub-contractors*) of this Schedule 34, the Supplier is entitled to sub-contract its obligations under this Schedule 34 to the TS Key Sub-contractors listed in the table below.
- 2 The Parties agree that they will update this Annex periodically to record any TS Key Sub-contractors appointed by the Supplier with the consent of the Authority after the Effective Date for the purposes of the delivery of the Transitional Services.



**ANNEX 11 (TS THIRD PARTY CONTRACTS) to
SCHEDULE 34 (TRANSITIONAL SUPPLIER)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 11

TS THIRD PARTY CONTRACTS

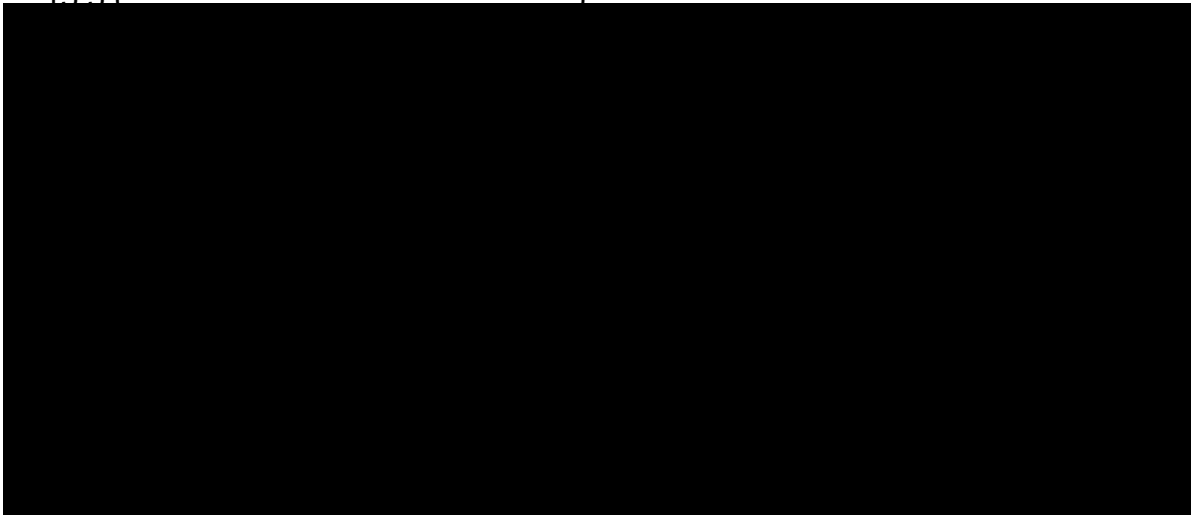
**ANNEX 11 (TS THIRD PARTY CONTRACTS) to
SCHEDULE 34 (TRANSITIONAL SUPPLIER)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Annex 11 (*TS Third Party Contracts*)

- 1 The contracts listed in the table below constitute TS Third Party Contracts entered into exclusively for the purposes of delivering the Transitional Services.
- 2 The Supplier shall be entitled to update this Annex in accordance with Clause 15.5 ()



**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 12
TS SOFTWARE

**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Annex 12 (*TS Software*)

1 THE TS SOFTWARE

- 1.1 The TS Software below is licensed to the Authority and/or the Service Recipients in accordance with Paragraph 16 (*TS Intellectual Property Rights*) and Annex 32 (*TS Intellectual Property Rights*).
- 1.2 The Parties agree that they will update this Annex regularly, and in any event no less than every 6 (six) Months from the Effective Date, to record any, Supplier Software or Third Party Software subsequently licensed by the Supplier or third parties for the purposes of the delivery of the Transitional Services.

**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

2 TS SUPPLIER SOFTWARE

The TS Supplier Software includes the following items:

Software	Supplier (if an Affiliate of the Supplier)	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non- COTS)	Term/Expiry
[REDACTED]							

**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

3 TS THIRD PARTY SOFTWARE

The TS Third Party Software shall include the following items:

TS Third Party Software	Supplier	Purpose	Number of Licences/ Users	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/Expiry
[REDACTED]							
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED]	[REDACTED]	1	[REDACTED]	1	[REDACTED]	[REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED]	[REDACTED]	1	[REDACTED]	1	[REDACTED]	[REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	1	[REDACTED]	1	[REDACTED]	[REDACTED]

**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

TS Third Party Software	Supplier	Purpose	Number of Licences/ Users	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/Expiry
[REDACTED]				[REDACTED]			[REDACTED]
[REDACTED] [REDACTED] [REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]

**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

TS Third Party Software	Supplier	Purpose	Number of Licences/ Users	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/Expiry
[REDACTED] [REDACTED] [REDACTED]				[REDACTED]			[REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED]		[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED] [REDACTED] [REDACTED]

**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

TS Third Party Software	Supplier	Purpose	Number of Licences/ Users	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/Expiry
[REDACTED] [REDACTED]							
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED] [REDACTED] [REDACTED]
[REDACTED]							
[REDACTED] [REDACTED] [REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]

**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

TS Third Party Software	Supplier	Purpose	Number of Licences/ Users	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/Expiry
[REDACTED] [REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED] [REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED] [REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]
[REDACTED] [REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

TS Third Party Software	Supplier	Purpose	Number of Licences/ Users	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/Expiry
[REDACTED]		[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED] [REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]							

**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

TS Third Party Software	Supplier	Purpose	Number of Licences/ Users	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/Expiry
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

TS Third Party Software	Supplier	Purpose	Number of Licences/ Users	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/Expiry
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

**APPENDIX 1: FORM OF LETTER RE SUB-LICENSING OF TS COTS SOFTWARE
AND TS COTS BACKGROUND IPRs**

[Supplier letterhead]

**[insert Authority or Service Recipient
name and address]**

[Date]

Dear Sirs

LICENCES FOR TS COTS SOFTWARE AND TS COTS BACKGROUND IPRs

We refer to the agreement between us dated **[insert date]** in respect of **[brief summary of subject of the Agreement]** (the “**Contract**”). Capitalised expressions used in this letter have the same meanings as in the Agreement.

In accordance with Paragraph 2.5(b) of Schedule 34 Annex 32 (*TS Intellectual Property Rights*) of the Contract we confirm that:

- 1 the **Authority / [name of Service Recipient]** is licensed by the Supplier to use the TS COTS Software and TS COTS Background IPRs identified in the first column of the Appendix to this letter (the “Appendix”) on the terms of the licences identified in the second column of the Appendix (the “Licences”); and
- 2 notwithstanding any provision to the contrary in the Licences, it is agreed that the **Authority / [name of Service Recipient]** may sub-licence, assign and novate the TS COTS Software and TS COTS Background IPRs as referred to in Paragraph 2.5(b) of Schedule 34 Annex 32 (*TS Intellectual Property Rights*) of the Contract.

Yours faithfully,

Signed:

On behalf of **[name of the Supplier]**

**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

APPENDIX 2: FORM OF CONFIDENTIALITY UNDERTAKING

CONFIDENTIALITY AGREEMENT

THIS AGREEMENT is made on **[date]** 20

BETWEEN:

- (1) **[insert name]** of **[insert address]** (the “**Sub-licensee**”); and
- (2) **[insert name]** of **[insert address]** (the “**Supplier**” and together with the Supplier, the “**Parties**”).

WHEREAS:

- (A) The Secretary of State for Justice of 102 Petty France, London, SW1H 2AJ (the “**Authority**”) and the Supplier are party to a contract dated **[insert date]** (the “**Contract**”) for the provision by the Supplier of **[insert brief description of services]** to the Authority **[and the]**.
- (B) The **Authority** wishes to grant a sub-licence to the Sub-licensee in respect of certain software and intellectual property rights licensed to the **Authority** pursuant to the Contract (the “**Sub-licence**”).
- (C) It is a requirement of the Contract that, before the **Authority** grants such sub-licence to the Sub-licensee, the Sub-licensee execute a confidentiality agreement in favour of the Supplier in or substantially in the form of this Agreement to protect the Confidential Information of the Supplier.

IT IS AGREED as follows:

1 Interpretation

1.1 In this Agreement, unless the context otherwise requires:

“Confidential Information”

means:

- (a) Information, including all personal data within the meaning of the Data Protection Act 2018, and however it is conveyed, provided by the **Authority** to the Sub-licensee pursuant to or in connection with the Sub-licence that relates to:
 - (i) the Supplier; or
 - (ii) the operations, business, affairs, developments, intellectual property rights, trade secrets, know-how and/or personnel of the Supplier;

**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (b) the source code and the object code of the software sub-licensed to the Sub-licensee pursuant to the Sub-licence together with build information, relevant design and development information, technical specifications of all functionality including those not included in standard manuals (such as those that modify system performance and access levels), configuration details, test scripts, user manuals, operating manuals, process definitions and procedures, and all such other documentation supplied by the Supplier to the **Authority** pursuant to or in connection with the Sub-licence;
- (c) other Information provided by the **Authority** pursuant to this Agreement to the Sub-licensee that is clearly designated as being confidential or equivalent or that ought reasonably to be considered to be confidential which comes (or has come) to the Sub-licensee's attention or into the Sub-licensee's possession in connection with the Sub-licence; and
- (d) Information derived from any of the above, but not including any Information that:
 - (a) was in the possession of the Sub-licensee without obligation of confidentiality prior to its disclosure by the **Authority**;
 - (b) was already generally available and in the public domain at the time of disclosure otherwise than by a breach of this Agreement or breach of a duty of confidentiality; or
 - (c) was independently developed without access to the Information;

“Information”

means all information of whatever nature, however conveyed and in whatever form, including in writing, orally, by demonstration, electronically and in a tangible, visual or machine-readable medium (including CD-ROM, magnetic and digital form); and

**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

“Sub-licence” has the meaning given to that expression in recital (B) to this Agreement.

1.2 In this Agreement:

- (a) a reference to any gender includes a reference to other genders;
- (b) the singular includes the plural and vice versa;
- (c) the words “include” and cognate expressions shall be construed as if they were immediately followed by the words “without limitation”;
- (d) references to any statutory provision include a reference to that provision as modified, replaced, amended and/or re-enacted from time to time (before or after the date of this Agreement) and any prior or subsequent subordinate legislation made under it;
- (e) headings are included for ease of reference only and shall not affect the interpretation or construction of this Agreement; and
- (f) references to Clauses are to clauses of this Agreement.

2 Confidentiality Obligations

2.1 In consideration of the **Authority** entering into the Sub-licence, the Sub- licensee shall:

- (a) treat all Confidential Information as secret and confidential;
- (b) have in place and maintain proper security measures and procedures to protect the confidentiality of the Confidential Information (having regard to its form and nature);
- (c) not disclose or permit the disclosure of any of the Confidential Information to any other person without obtaining the prior written consent of the Supplier or except as expressly set out in this Agreement;
- (d) not transfer any of the Confidential Information outside the United Kingdom;
- (e) not use or exploit any of the Confidential Information for any purpose whatsoever other than as permitted under the Sub-licence;
- (f) immediately notify the Supplier in writing if it suspects or becomes aware of any unauthorised access, copying, use or disclosure in any form of any of the Confidential Information; and
- (g) upon the expiry or termination of the Sub-licence:

**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (i) destroy or return to the Supplier all documents and other tangible materials that contain any of the Confidential Information;
- (ii) ensure, so far as reasonably practicable, that all Confidential Information held in electronic, digital or other machine-readable form ceases to be readily accessible (other than by the information technology staff of the Sub-licensee) from any computer, word processor, voicemail system or any other device; and
- (iii) make no further use of any Confidential Information.

3 Permitted Disclosures

- 3.1 The Sub-licensee may disclose Confidential Information to those of its directors, officers, employees, consultants and professional advisers who:
 - (a) reasonably need to receive the Confidential Information in connection with the Sub-licence; and
 - (b) have been informed by the Sub-licensee of the confidential nature of the Confidential Information; and
 - (c) have agreed to terms similar to those in this Agreement.
- 3.2 The Sub-licensee shall be entitled to disclose Confidential Information to the extent that it is required to do so by applicable law or by order of a court or other public body that has jurisdiction over the Sub-licensee.
- 3.3 Before making a disclosure pursuant to Clause 3.2, the Sub-licensee shall, if the circumstances permit:
 - (a) notify the Supplier in writing of the proposed disclosure as soon as possible (and if possible before the court or other public body orders the disclosure of the Confidential Information); and
 - (b) ask the court or other public body to treat the Confidential Information as confidential.

4 General

- 4.1 The Sub-licensee acknowledges and agrees that all property, including intellectual property rights, in Confidential Information disclosed to it by the Supplier shall remain with and be vested in the Supplier.
- 4.2 This Agreement does not include, expressly or by implication, any representations, warranties or other obligations:
 - (a) to grant the Sub-licensee any licence or rights other than as may be expressly stated in the Sub-licence;

**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- (b) to require the Supplier to disclose, continue disclosing or update any Confidential Information; or
 - (c) as to the accuracy, efficacy, completeness, capabilities, safety or any other qualities whatsoever of any Information or materials provided pursuant to or in anticipation of the Sub-licence.
- 4.3 The rights, powers and remedies provided in this Agreement are cumulative and not exclusive of any rights, powers or remedies provided by law. No failure or delay by either Party to exercise any right, power or remedy will operate as a waiver of it nor will any partial exercise preclude any further exercise of the same, or of some other right, power or remedy.
- 4.4 Without prejudice to any other rights or remedies that the Supplier may have, the Sub-licensee acknowledges and agrees that damages alone may not be an adequate remedy for any breach by the Sub-licensee of any of the provisions of this Agreement. Accordingly, the Sub-licensee acknowledges that the Supplier shall be entitled to the remedies of injunction and specific performance as well as any other equitable relief for any threatened or actual breach of this Agreement and/or breach of confidence and that no proof of special damages shall be necessary for the enforcement of such remedies.
- 4.5 The maximum liability of the Sub-licensee to the Supplier for any breach of this Agreement shall be limited to ten million pounds (£10,000,000).
- 4.6 For the purposes of the Contracts (Rights of Third Parties) Act 1999 no one other than the Parties has the right to enforce the terms of this Agreement.
- 4.7 Each Party shall be responsible for all costs incurred by it or on its behalf in connection with this Agreement.
- 4.8 This Agreement may be executed in any number of counterparts and by the Parties on separate counterparts, but shall not be effective until each Party has executed at least one counterpart. Each counterpart shall constitute an original of this Agreement, but all the counterparts shall together constitute but one and the same instrument.

5 Notices

- 5.1 Any notice to be given under this Agreement (each a “**Notice**”) shall be given in writing and shall be delivered by hand and shall be deemed to have been duly given at the time of delivery provided that such Notice is sent to the relevant physical address, and expressly marked for the attention of the relevant individual, set out in Clause 5.2.
- 5.2 Any Notice:
- (a) if to be given to the Supplier shall be sent to:

[Address]Attention: **[Contact name and/or position, e.g. “The Finance Director”]**

**ANNEX 12 (TS SOFTWARE) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

(b) if to be given to the Sub-licensee shall be sent to:

[Name of Organisation]

[Address]

Attention: [REDACTED]

6 Governing law

- 6.1 This Agreement shall be governed by, and construed in accordance with, English law and any matter claim or dispute arising out of or in connection with this Agreement whether contractual or non-contractual, shall be governed by and determined in accordance with English law.
- 6.2 Each Party hereby irrevocably submits to the exclusive jurisdiction of the English courts in respect of any claim or dispute arising out of or in connection with this Agreement.

IN WITNESS of the above this Agreement has been signed by the duly authorised representatives of the Parties on the date which appears at the head of page 1.

For and on behalf of [name of Supplier]

Signature:

Date:

Name:

Position:

For and on behalf of [name of Sub-licensee]

Signature:

Date:

Name:

Position:

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 15

TS CHARGES AND INVOICING

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

1. PURPOSE OF THIS ANNEX

1.1 This Annex 15 (*TS Charges and Invoicing*) sets out the provisions relating to:

- 1.1.1 key Charges principles;
- 1.1.2 TS Milestone Payments;
- 1.1.3 TS Service Charges;
- 1.1.4 Charges for TS Projects;
- 1.1.5 TS Delay Payments
- 1.1.6 TS Service Credits;
- 1.1.7 Certification of TS Costs; and
- 1.1.8 invoicing.

2. KEY CHARGING PRINCIPLES

- 2.1 Other than as expressly stated in this Schedule 34 the Supplier is not entitled to any form of payment in addition to, or any amendment to, the TS Charges whether as a result of increased costs, expenses, risks or any other matter.
- 2.2 The TS Charges set out or referred to in this Annex 15 (*TS Charges and Invoicing*) are the only charges that the Supplier can charge for the provision of the Transitional Services. No additional fees, charges or expenses shall be payable by the Authority to the Supplier in addition to those set out or referred to in this Annex 15 (*TS Charges and Invoicing*).
- 2.3 The Supplier acknowledges that the Authority needs visibility of the Transitional Supplier's costs to understand any payment sought by the Supplier and to agree the impact of any TS Contract Change or TS Project Work Order. Accordingly, the Supplier shall:
 - 2.3.1 make available to the Authority only its estimations and projections of future costs and charges and its records and accounts of all actual costs and charges relating to the Transitional Services (including in respect of any TS Contract Change or TS Project) in accordance with the financial transparency requirements referred to in Paragraph 2.3.2;
 - 2.3.2 comply with the following financial transparency requirements:

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

2.3.2.1 Schedule 19 (*Financial Reports and Audit Rights*); and

2.3.2.2 Paragraph 7 (*Certification of TS Costs*) of this Annex 15.

2.4 Any variation to the TS Charges shall only apply if agreed in writing and in advance in accordance with the Change Control Procedure.

2.5 If the Supplier fails to comply with Paragraph 10 (*Payment Planner*) of this Annex 15, the Authority reserves the right to withhold payment of any TS Charges due and payable under this Schedule 34.

2.6 All TS Charges set out in this Annex 15 (*TS Charges and Invoicing*) are exclusive of VAT.

2.7 Any amounts or sums in this Schedule 34 which are expressed to be "subject to Indexation" shall be adjusted in accordance with the provisions of Paragraph 2.8 to reflect the effects of inflation.

2.8 Where Indexation applies, the relevant adjustment shall be:

2.8.1 if the Effective Date is:

2.8.1.1 on or after 1 April and on or before 31 December in the same calendar year, applied on the first anniversary of the Effective Date and each subsequent anniversary of the Effective Date thereafter; or

2.8.1.2 not within the period set out in paragraph 2.8.1.1, applied on the first day of the second April following the Effective Date, and on the first day of April in each subsequent year (each such date an "**adjustment date**");

2.8.2 for TS Charges in the TS Rate Card set out in Appendix D (*TS Rate Card*), determined by multiplying the relevant amount or sum by the percentage increase or changes in the Average Weekly Earnings Index (EARN01) published by the Office of National Statistics for (a) where Paragraph 2.8.1.1 applies, the 12 months ended on the last day of the month preceding the anniversary of the Effective Date for which this index has been officially published; or (b) where Paragraph 2.8.1.2 applies, the 12 months ended on the 31 January immediately preceding the relevant adjustment date; and

2.8.3 for all other TS Charges stated to be subject to Indexation, determined

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

by multiplying the relevant amount or sum by the percentage increase or changes in the Consumer Price Index (CPI) published by the Office of National Statistics for (a) where Paragraph 2.8.1.1 applies, the 12 months ended on the last day of the month preceding the anniversary of the Effective Date for which this index has been officially published; or (b) where Paragraph 2.8.1.2 applies, the 12 months ended on the 31 January immediately preceding the relevant adjustment date.

- 2.9 Notwithstanding Paragraph 2.1, where the Supplier's costs increase owing to price changes by Sub-contractors beyond the Supplier's control and where the Supplier can show to the Authority's reasonable satisfaction that the Supplier cannot avoid such price increase, the Supplier may submit a Change Request and the Change Control Procedure shall apply.
- 2.10 Except as set out in Paragraph 2.7, Paragraph 2.9 and/or Paragraph 2 of Appendix B to this Annex 15, neither the TS Charges nor any other costs, expenses, fees or charges shall be adjusted to take account of any inflation, change to exchange rate, change to interest rate or any other factor or element which might otherwise increase the cost to the Supplier or Sub-contractors of the performance of their obligations.

3. TS SERVICE CHARGES

- 3.1 The Authority will pay the TS Service Charges to the Supplier for all Transitional Services in each Service Period from the Effective Date to the end of the TS Term. The TS Service Charges shall be made up of:
- 3.1.1 the monthly service charges calculated in accordance with Appendix B to this Annex 15 (the "**Monthly TS Service Charges**"); and
- 3.1.2 TS Charges for products and services provided from the TS Product and Service Catalogue as set out in Appendix C to this Annex 15 (*TS Charges and Invoicing*) and as may be amended from time to time by the Parties in accordance with Schedule 22 (*Change Control Procedure, Service Requests and Projects*),

less any TS Service Credits payable in accordance with Paragraph 6 below.

- 3.2 Either Party may propose TS Changes in accordance with the Change Control Procedure which impact upon the TS Service Charges. The Parties acknowledge that a TS Change to the TS Service Charges may impact upon the people cost element of the TS Service Charges. The Supplier agrees that if any such proposed TS Change has an impact upon the people cost element of

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

the TS Service Charges, any proposed changes to the people cost element shall be calculated by reference to the TS Rate Card in Appendix D to this Annex 15.

3.3 The TS Service Charges will be payable monthly in arrears in accordance with Paragraph 8 of this Annex 15 (*TS Charges and Invoicing*).

3.4 Not used.

3.5 Not used.

3.6 The Supplier acknowledges and agrees that the Authority gives no warranty or representation as to:

3.6.1 the number or volume of units consumed or required in the performance of the Transitional Services; and/or

3.6.2 the total TS Service Charges.

3.7 The Supplier shall provide the Authority with sufficient evidence to enable the Authority to determine and verify the amount of units consumed and the amount of TS Service Charges which are payable.

TS Product and Service Catalogue

3.8 The TS Product and Service Catalogue shall list the services and goods and associated charges that the Parties have agreed can be ordered by the Authority. This shall include Transitional Services that are paid for through the TS Charges, or other agreed charges.

3.9 If services are added to the TS Product and Service Catalogue, the charges associated with each product and/or service package shall be determined at the time that it is added in accordance with Schedule 22 (*Change Control Procedure, Service Requests and Projects*) and the relevant charges shall be set out in the TS Product and Service Catalogue.

3.10 The TS Charges for services and goods in the TS Product and Service Catalogue shall not be subject to Indexation.

4. CHARGES FOR TS CHANGES, TS SERVICE REQUESTS AND TS PROJECTS**Rate Cards**

4.1 If the Parties agree that the Supplier shall provide ad-hoc Transitional Services

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

or a TS Project (together, the “**TS Rate Card Services**”), then the TS Charges for such TS Rate Card Services shall be payable on the basis of the charging mechanism set out in the relevant Project Work Order (for a TS Project) or Service Request.

- 4.2 The charging mechanism may specify that TS Charges are to be payable on the basis of TS Milestone Payments or TS Time and Materials Charges, in addition to or instead of any TS Service Charges. People cost elements of the TS Charges for such TS Rate Card Services shall be calculated on a daily basis for every Person Day that the agreed Supplier Personnel are actively performing the TS Rate Card Services by reference to the TS Project Daily Rate by role in the TS Rate Card set out in Appendix D to this Annex 15 (*TS Charges and Invoicing*) and shall be inclusive of Reimbursable Expenses (unless otherwise agreed by the Authority). The TS Rate Card shall be subject to Indexation.

TS Milestone Payments

- 4.3 The Parties may specify TS Milestone Payments as the charging basis for part or all of a TS Project.
- 4.4 TS Project Work Orders that specify TS Charges payable on the basis of TS Milestone Payments shall set out the details of each TS Milestone Payment, including the Milestone Date, amount payable and value of any retention or TS Delay Payment (if applicable).
- 4.5 The Supplier shall be entitled to deliver an invoice to the Authority in respect of each TS Milestone Payment:
- 4.5.1 on the issue by the Authority of a Milestone Achievement Certificate in accordance with Schedule 14 (*Testing Procedures*); or
- 4.5.2 on the Supplier Achieving and evidencing the agreed Acceptance Criteria to the Authority’s reasonable satisfaction as set out in a Project Work Order,
- for the TS Milestone associated with that TS Milestone Payment.
- 4.6 The circumstances in which a TS Milestone shall be considered to have been Achieved are set out in the relevant Project Work Order. Payment shall be made to the Supplier in accordance with Paragraph 8 of this Annex 15.
- 4.7 Unless otherwise agreed in the TS Project Work Order, TS Milestone Payments shall constitute full consideration for the TS Project and shall be fully inclusive

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

of all costs and expenses incurred in performance of the applicable TS Project.
The TS Milestone Payments shall not be subject to Indexation.

TS Time and Material Charges

- 4.8 Where the Project Work Orders for a TS Project specifies time and materials charges ("**TS Time and Materials Charges**") for Person Day Resources, such TS Time and Materials Charges shall be calculated each month as the aggregate of Person Day Resources and Reimbursable Expenses consumed in delivering the relevant TS Project in that month:

4.8.1 where Person Day Resources are calculated by reference to:

- (a) the number of Person Days utilised for each grade of Supplier Personnel in that month; and
- (b) the TS Project Daily Rate applicable to the relevant grade of Supplier Personnel.

provided that where Supplier Personnel work less than a full Person Day, the relevant charge shall be calculated based on the applicable TS Project Daily Rate pro rata for each whole hour worked; and

4.8.2 Reimbursable Expenses in respect of a TS Project must:

- (a) be agreed and authorised by the Authority in advance of performing the relevant Transitional Services;
- (b) be calculated at the rates and in accordance with the Authority's expenses policy current from time to time;
- (c) be incurred as a result of Supplier Personnel performing the Transitional Services at a location which is away from their usual place of work at the Supplier's or Transitional Supplier's or relevant Sub-contractor's offices and not at the Authority premises stated on the Project Work Order or Service Request as being the location(s) for delivery of the TS Project; and
- (d) be supported by appropriate documentary evidence of such expenses being incurred.

- 4.9 No finance charges, risks or contingencies or any other uplifts shall be applied to the TS Time and Materials Charges.

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 4.10 The Supplier shall maintain full and accurate records of the time spent by the Supplier's Personnel in providing the Transitional Services and shall provide such records to the Authority with each relevant invoice submitted in accordance with Paragraph 8 of this Annex 15 (*TS Charges and Invoicing*).

Utilisation Discount

- 4.11 In respect of TS Rate Card Services, the Supplier shall discount the applicable TS Project Daily Rates, in accordance with Paragraph 4.12, to reflect the benefit to the Supplier of long-term deployments of Supplier Personnel.
- 4.12 If the parties agree that the Supplier shall provide TS Rate Card Services by deploying Supplier Personnel for any of the periods of deployment set out in Table 2 in Appendix D to this Annex 15, the Supplier shall discount the applicable TS Project Daily Rate by role for each applicable Supplier Personnel by reference to the corresponding "Utilisation Discount" column of Table 2 in Appendix D to this Annex 15.

Volume Rebate

- 4.13 In respect of any TS Charges for TS Rate Card Services that are invoiced to the Authority in any Contract Year, the Supplier shall pay to the Authority (or issue a credit note of equivalent value) a sum calculated by reference to the bandings in the rows of the "Value (£) invoiced in Contract Year" column and the percentages in the "Rebate %" column of Table 3 in Appendix D to this Annex 15.

Charges for TS Changes – other requirements

- 4.14 Where either Party requests a TS Change, then the Supplier shall assess the potential impact of the proposed TS Change on the TS Charges in accordance with the TS Change Control Procedure. Without limiting Paragraph 5 (*Impact Assessment*) of Part A (*Change Control Procedure*) of Schedule 22 (*Change Control Procedure, Service Requests & Projects*), the Supplier shall provide sufficient detail to justify the potential impact on the TS Changes which shall:
- 4.14.1 be based on and reflect the principles of the TS Financial Model;
 - 4.14.2 include estimated volumes of each type of resource to be employed using the applicable "TS Project Daily Rate" set out in Appendix D to this Annex 15;
 - 4.14.3 include full disclosure of any assumptions underlying the proposed impact on the TS Changes; and

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

- 4.14.4 include evidence of the cost of any assets required for the proposed TS Change in accordance with Paragraphs 5.5(e) and 5.6 of Part A of Schedule 22 (*Change Control, Service Requests & Projects*).
- 4.15 The Supplier may not charge for the development of commercial proposals, estimates, financial impact assessments or quotations for the Supplier to undertake work for the Authority and such activities shall be non-chargeable.
- 4.16 If the proposed Contract Change is approved by the Authority in accordance with the Change Control Procedure, then the Supplier will update the TS Financial Model in accordance with the provisions of Schedule 19 (*Financial Reports and Audit Rights*).
- 4.17 The Supplier shall use the TS Financial Model to demonstrate any proposed revisions to the TS Charges arising as a result of any proposed TS Change.
- 4.18 Unless otherwise specified by the Authority, the Supplier shall provide to the Authority estimates of any proposed charges for a proposed work package or project in terms of TS Milestone Payments.
- 4.19 The Authority reserves the right to require Project Work Orders to include provisions for TS Delay Payments.

TS Project Contingency and Risk

- 4.20 Where TS Projects are charged on a fixed price basis with payments linked to TS Milestones, the Supplier may include an appropriate level of contingency and risk premium within the agreed price. To ensure that the Authority has transparency over the contingencies added, and that risks are not double counted, the Supplier shall ensure that the following principles for costing contingency and risk shall be applied:
- 4.20.1 the day effort calculated by the Supplier excluding any contingency or risk premiums;
- 4.20.2 contingency shall be calculated as a percentage of the total person-day effort to reflect the level of uncertainty (estimating risk) in the person-day estimates. This percentage will be agreed between the Authority and the Supplier and will be informed by such factors as: the precision of the project specification and outputs; completeness of information; availability of accurate metrics; the complexity of the solution; feedback from relevant completed projects and the period of time over which the project is delivered;

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 4.20.3 Outline TS Project Plans will then be presented by the Supplier that reflect the level of person-days and timescales for milestones and deliverables inclusive of the agreed contingency;
- 4.20.4 a TS Risk Register shall be presented by the Supplier which identifies all TS Project specific risks, an estimate of the value of the risk if it were to materialise, planned actions to mitigate the risk, cost of implementing such actions and an estimate of the residual value of the risk after the mitigating actions have been taken;
- 4.20.5 the quantification of risk values shall take account of those risks that are independent of each other and those risks that are interdependent. The cumulative value of the interdependent risk values should be less than the sum of each individual risk to reflect the direct relationship between each risk;
- 4.20.6 prior to agreeing the fixed charges for a TS Project, the Supplier shall endeavour to minimise the likelihood of identified risks materialising, to ensure any risk premium value is kept to a minimum. Such actions could include detailed scoping studies, business impact analysis, pilot and testing activities;
- 4.20.7 any agreed residual risk value of risks owned by the Supplier shall be included in the project costing, but not converted into person-day effort within the project plans; and
- 4.20.8 the utilisation of project contingency and risk premiums shall be measured and shared with the Authority on a transparent basis. The outcomes shall be fed back into future project costing to continuously improve the accuracy of the project estimating process.

Capital and 3rd Party Project Costs

- 4.21 If any TS Projects require the Supplier to procure services or capital assets from third parties on a pass-through basis, the Supplier shall not mark-up the costs charged by such third parties to the Supplier by more than 0% in its pass-through charge to the Authority.

5. TS DELAY PAYMENTS

- 5.1 As part of agreeing any TS Contract Change or TS Project, the Parties may agree to apply TS Delay Payments.

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 5.2 If the Authority and the Supplier are unable to agree on the arrangements for the TS Delay Payments, the Parties shall refer the matter to the Dispute Resolution Procedure in accordance with Schedule 23 (*Dispute Resolution Procedure*).
- 5.3 TS Delay Payments shall, unless otherwise agreed in the Project Initiation Process (as defined in Paragraph 4.1 of Part B (*Service Requests and Projects*) of Schedule 22 (*Change Control Procedure, Service Requests and Projects*)), follow the provisions of this Schedule 34 including this Paragraph 5.
- 5.4 If a TS Milestone has not been Achieved by the relevant Milestone Date, the Supplier shall pay to the Authority TS Delay Payments for each day of delay from and including the relevant Milestone Date until and including the earlier of:
- 5.4.1 the date on which the Authority provides the Supplier with a Milestone Achievement Certificate; and
- 5.4.2 the expiry of the TS Delay Deduction Period.
- 5.5 For avoidance of doubt, the TS Delay Payment shall be the Authority's exclusive financial remedy for the Supplier's failure to Achieve a TS Milestone by its Milestone Date except where the Delay exceeds the TS Delay Deduction Period and the Authority reserves its rights and remedies in such circumstances.
- 5.6 If no further TS Milestone Payments fall due in relation to a TS Project after TS Delay Payments accrue, the Supplier shall issue a credit note to the Authority and a sum equal to any such TS Delay Payments then outstanding shall be repayable by the Supplier to the Authority as a debt.
- 5.7 Dates and amounts of the TS Delay Payments and any cap on the TS Delay Payments shall be set out in the relevant Project Work Order. Such TS Delay Payments should represent a genuine pre-estimate of the loss likely to be suffered by the Authority as a result of the applicable delay.
- 6. TS SERVICE CREDITS**
- 6.1 TS Service Credits will be calculated based on the number of TS Service Credit Points accrued in any one Service Measurement Period. The basis for the accrual of TS Service Credit Points is set out in Annex 3 (*TS Performance Levels*).
- 6.2 In each Service Measurement Period, subject to the cap set out in Paragraph 6.3, the TS Service Credit deduction will be equal to the Total TS Service Credit

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Points for the Service Measurement Period ('**TSCP**') multiplied by twenty per cent (20%) of the Applicable TS Charge divided by the Maximum TS Service Credit Points to Reach Cap. The total TS Service Credit applicable for each Service Measurement Period will therefore be calculated in the following way:

$$\text{TSSC} = \text{TSCP} \times 20\% \text{ of the Applicable TS Charge} / \text{Maximum TS Service Credit Points to Reach Cap}$$

Where:

"Applicable TS Charge" = TS Service Charges payable for the relevant Service Measurement Period

"TSSC" = TS Service Credit

"TSCP" = Total TS Service Credit Points for the Service Measurement Period

"Maximum TS Service Credit Points to Reach Cap" = 5,000

- 6.3 The liability of the Supplier for TS Service Credits for each Service Measurement Period will be limited to twenty per cent (20%) of the Applicable TS Charge (the **"TS Service Credit Cap"**). However, and for the avoidance of doubt, such TS Service Credit Cap shall not affect the continued accrual of TS Service Credit Points in excess of such TS Service Credit Cap, in accordance with the provisions of Annex 3 (*TS Performance Levels*).
- 6.4 If no further TS Charges fall due after TS Service Credits accrue, the Supplier shall issue a credit note to the Authority for a sum equal to any such TS Service Credits then outstanding which shall be repayable by the Supplier to the Authority as a debt.
- 6.5 The Authority may review the Maximum TS Service Credit Points to Reach Cap from time to time in accordance with paragraph 1.3 of Annex 3 (*TS Performance Levels*).

7. CERTIFICATION OF TS COSTS

- 7.1 The Supplier shall as part of a financial Audit pursuant to Part C of Schedule 19 (*Financial Reports and Audit Rights*) within 15 Working Days of such request provide to the Authority a certificate of costs incurred by the Supplier in providing the Transitional Services in the format as set out in Appendix A to this Annex 15 (*TS Charges and Invoicing*) ("**Certificate of TS Costs**") (such requests not to exceed five occasions over the TS Term). The Certificate of TS Costs shall be signed by a director of the Transitional Supplier.

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 7.2 The Certificate of TS Costs shall set out the Transitional Supplier's actual costs, expenses and profits in providing the Transitional Services over the preceding year of this Contract, including details of at least the following:
- 7.2.1 the actual capital expenditure, including capital replacement costs (including details of expected asset lives);
 - 7.2.2 actual operating expenditure relating to the provision of the Transitional Services, with labour costs, consumables, sub-contracted and bought-in services;
 - 7.2.3 all interest expenses and other third party financing costs;
 - 7.2.4 details of the overhead recoveries that have been made to the extent detailed in Appendix A to this Annex 15 (*TS Charges and Invoicing*); and
 - 7.2.5 the profit which the Transitional Supplier has achieved in the provision of the Transitional Services including any profit element forming any part of the overhead recoveries disclosed by reason of Paragraph 7.2.4 above.
- 7.3 Following receipt of the Certificate of TS Costs, the Supplier shall provide to the Authority any reasonable additional information to enable the Authority to verify the accuracy of the Certificate of TS Costs.
- 7.4 Following receipt of the Certificate of TS Costs, the Authority (and its expert third party advisors) shall be entitled at any time to access the Transitional Supplier's computations that have been used by the Transitional Supplier in the preparation of the Certificate of TS Costs. The computations should follow the visibility principles set out in Paragraph 3 of Schedule 19 (*Financial Reports and Audit Rights*).
- 8. INVOICING**
- 8.1 The Supplier shall prepare and provide to the Authority for Approval a draft pro forma invoice within ten (10) Working Days (or such other period as the Parties agree in writing) of the Effective Date which shall include, as a minimum, the details set out in Paragraph 8.3 below together with such other information as the Authority may reasonably require. If the draft pro forma invoice is not Approved by the Authority, then the Supplier shall make such amendments as may be reasonably required by the Authority.

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

8.2 Raising Invoices

8.2.1 Subject to Paragraph 8.2.2, the Supplier shall be entitled to raise an invoice in respect of any payment as agreed through the Payment Planner review process as described in Paragraph 10 below and which is payable to the Supplier pursuant to this Schedule 34 provided that each invoice is delivered to the Authority within ten (10) Working Days after either:

8.2.1.1 the date on which the Milestone Achievement Certificate is issued in relation to a TS Milestone; or

8.2.1.2 the end of the month in which the TS Service Charges have been incurred.

8.2.2 The Supplier shall either:

8.2.2.1 submit all invoices to the Authority in the same financial year (1 April to 31 March) that the Transitional Services to which the invoice relates were delivered; or

8.2.2.2 where it is not reasonably practicable for the Supplier to submit an invoice in accordance with Paragraph 8.2.2.1, provide confirmation of the agreed forecasted amount that will be invoiced for such Transitional Services to the Authority.

8.2.3 The Supplier shall submit all invoices and address any invoice queries to the Authority's contract manager. The address will be as notified by the Authority to the Supplier from time to time.

8.2.4 not used

8.2.5 not used

8.2.6 not used

8.2.7 The Supplier's finance director (or equivalent) shall provide a letter addressed to the Authority no later than ten (10) Working Days before the end of the relevant Authority financial year (1 April to 31 March), confirming that:

8.2.7.1 TS Charges for all Transitional Services provided under this Schedule 34 up until the end of month eleven (11) for the

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

relevant Authority financial year, have been properly invoiced in accordance with this Paragraph 8; or

8.2.7.2 TS Charges for all Transitional Services provided under this Schedule 34 up until the end of month eleven (11) for the relevant Authority financial year, have been invoiced in accordance with this Paragraph 8 apart from those specifically identified as not invoiced in the letter, such information to provide sufficient detail of the Transitional Services that are yet to be invoiced to enable the Authority to make a reasonable estimate of charges which are likely to be invoiced including: (i) details of the relevant Transitional Services, (ii) the reasons why this information cannot be provided for these Transitional Services, (iii) where known, an estimate of the level of TS Charges to be invoiced for these Transitional Services, and (iv) proposals for resolving the issues and proposed timescales for invoicing the TS Charges for these Transitional Services.

8.2.8 The Parties shall work together in good faith to agree a plan to resolve the issues raised under Paragraph 8.2.7 and agree a timetable for invoicing these services. In the event that the Parties fail to agree such a plan and timetable within thirty (30) days of the date of the letter or the Supplier fails to implement the agreed actions within the agreed timescales then the Supplier shall only be entitled to raise an invoice for charges related to such services in accordance with the process described in Paragraph 8.2.9.

8.2.9 The Supplier shall only be entitled to raise an invoice in respect of an uninvoiced charge (whether discovered as an underpayment via an audit undertaken by the Authority, or otherwise) where the Supplier has notified and/or invoiced the Authority for such TS Charges in accordance with Paragraph 8.2.2. Invoices delivered which relate to uninvoiced charges that have not been invoiced or notified to the Authority in accordance with Paragraph 8.2.2 shall be invalid and the Authority shall have no liability in respect of such invoices.

8.3 Format of invoice

8.3.1 The Supplier shall ensure that each invoice contains the following information:

8.3.1.1 the date the invoice is issued and if date of supply is different from issue date, need to add tax point date;

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 8.3.1.2 a unique invoice number;
- 8.3.1.3 details of the correct contract reference with description;
- 8.3.1.4 clear description of what Transitional Services, TS Changes, TS Catalogue Items or other service or goods to which each element of the TS Charges refers;
- 8.3.1.5 the date or period(s) to which the relevant TS Charges relate (supply date);
- 8.3.1.6 the purchase order number and requester name and TS Milestone reference to which it relates (if any);
- 8.3.1.7 a copy of the relevant information from the Payment Planner (to be displayed on the front page of the invoice);
- 8.3.1.8 the dates between which the Transitional Services the subject of each of the TS Charges detailed on the invoice were performed;
- 8.3.1.9 the methodology applied to calculate the TS Charges (namely whether the TS Charges are calculated on a fixed price basis, time and materials basis, or other basis);
- 8.3.1.10 the total TS Charges gross and net of any applicable deductions/discounts and, separately, the amount of any disbursements properly chargeable to the Authority under the terms of this Schedule 34, and, separately, any VAT or other sales tax payable in respect of the same;
- 8.3.1.11 details of any TS Service Credits or similar deductions that shall apply to the TS Charges detailed on the invoice;
- 8.3.1.12 a contact name and telephone number/email of a responsible person in the Supplier's finance department in the event of administrative queries;
- 8.3.1.13 the bank account details for payments to the Supplier via electronic transfer of funds (i.e. name and address of bank, sort code, account name and number); and
- 8.3.1.14 to specify the payment terms clearly on the invoice.

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 8.3.2 Each invoice shall at all times be supported by sufficient information ("**TS Supporting Information**"), to enable the Authority to reasonably assess whether the TS Charges detailed thereon are properly payable. Any assessment by the Authority of the TS Supporting Information shall not be conclusive. The Supplier undertakes to provide to the Authority any other documentation reasonably required by the Authority from time to time to substantiate an invoice including information required to enable the Authority to internally or externally cross charge.
- 8.3.3 The Supplier shall submit all invoices and TS Supporting Information in such format as the Authority may specify from time to time:
- 8.3.3.1 by post to: SSCL – MoJ PO Box 743, Newport, NP10 8FZ
- 8.3.3.2 by email as unstructured electronic invoices in pdf format to 8FZ APinvoices-MOJ-U@gov.sscl.com email address.
- 8.3.3.3 to such other address, whether physical or electronic, as may be notified by the Authority in accordance with Paragraph 8.2.3.
- 8.3.4 All Supplier invoices shall be expressed in sterling or such other currency as shall be permitted by the Authority in writing.
- 8.3.5 The Authority shall only regard an invoice as valid if it complies with the provisions of this Annex 15 (*TS Charges and Invoicing*). Where any invoice does not conform to the Authority's requirements set out in Paragraph 8.3 of this Annex 15 (*TS Charges and Invoicing*), the Authority will promptly return the disputed invoice to the Supplier. The Supplier shall promptly issue a replacement invoice which shall comply with the same.
- 8.3.6 The final invoice(s) relating to this Schedule 34 shall only be sent to the Authority following agreement between the Parties, such agreement not to be unreasonably withheld or delayed, of any TS Service Credits relating to the TS Service Credit regime as detailed in Annex 3 (*TS Performance Levels*).

Electronic Invoicing

- 8.3.7 The Authority shall accept and process for payment an electronic invoice submitted for payment by the Supplier where the invoice is undisputed and where it complies with the standard on electronic invoicing.

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

8.3.8 For the purposes of Paragraph 8.3.7, an electronic invoice complies with the standard on electronic invoicing where it complies with the European standard and any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870.

8.4 TS Supporting information

8.4.1 TS Milestone Payments must be supported by copies of Milestone Achievement Certificates as signed by appropriately authorised Authority personnel.

8.4.2 Except where Paragraph 8.4.3 applies, any items ordered through the TS Product and Service Catalogue can be aggregated on an invoice, subject to all orders being raised under the same purchase order number but shall be supported by individual order and delivery information, including organisation, authorisation and budgetary code information. This has to be sufficient to enable re-charges to be made within the Authority and associated bodies. TS Charges for orders not containing sufficient information to enable re-charge will be disputed.

8.4.3 Each invoice will only be paid if the amount matches the amount agreed through the Payment Planner process as detailed in Paragraph 10 below.

8.5 Payment terms

8.5.1 The Authority shall pay undisputed valid invoices within thirty calendar (30) days of receipt.

8.6 Credit notes

8.6.1 The Supplier shall provide the Authority with a credit note in the following circumstances:

8.6.1.1 an invoice in full or in part has been issued in error with reason for credit;

8.6.1.2 the agreed resolution of a disputed invoice is that the disputed charge is too high and a credit note is agreed to be issued;

8.6.1.3 the Authority is eligible to receive TS Delay Payments and has requested that the TS Delay Payments are realised by a credit note;

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

8.6.1.4 the Authority is eligible to receive TS Service Credits and has requested that the TS Service Credits are realised by a credit note; and

8.6.1.5 other circumstances as agreed between the Authority and the Supplier.

8.6.2 Each credit note shall be a valid tax invoice and shall be issued promptly by the Supplier and in any event no later than the end of the next month following agreement between the Parties for the provision of a credit note due to the occurrence of any of the circumstances set out in Paragraph 8.6.1 above.

8.7 Disputed invoices

8.7.1 If the Authority disputes all or part of an invoice raised by the Supplier, then the Authority shall inform the Supplier at the earliest opportunity. The Authority shall set out the nature of the dispute and reasons for the dispute.

8.7.2 At its sole discretion, the Authority may postpone payment of the disputed amount until the dispute is resolved and any correcting documentation (further invoice or credit note) has been received.

8.7.3 Where the disputed amount is a part of a larger invoice, the entire invoice will be disputed. The Authority will not part pay an invoice.

8.7.4 Payment by the Authority of any invoice submitted by the Supplier shall not signify approval of such invoice. The Authority reserves the right to verify and, where appropriate, dispute invoices after the date of payment and subsequently to recover any sums which have been overpaid.

8.7.5 If any part of an invoice rendered by the Supplier is disputed or subject to question by the Authority either before or after payment then the Authority may call for the Supplier to provide such further documentary evidence as it may reasonably require to verify its liability to pay the amount which is disputed or subject to question and the Supplier shall promptly provide such evidence in a form satisfactory to the Authority.

8.7.6 For the avoidance of doubt, where a disputed invoice has not been resolved and has been referred to the Dispute Resolution Procedure, the Supplier may invoice the Authority for the Transitional Services that have been provided and are not in Dispute.

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

9. MANAGEMENT CHARGES AND INFORMATION

9.1 In addition to any other management information requirements set out in this Schedule 34, the Supplier agrees and acknowledges that it shall at no charge, provide timely, full, accurate and complete SME Management Information (MI) reports to the Authority which incorporate as a minimum the following data:

9.1.1 the total contract revenue received directly on a specific contract;

9.1.2 the total value of sub-contracted revenues under the contract (including revenues for non-SMEs/non-VCSEs); and

9.1.3 the total value of sub-contracted revenues to SMEs and VCSEs.

9.2 The SME Management Information Reports shall be provided in such format as is reasonably requested by the Authority and any guidance issued by the Authority from time to time. The Authority shall give at least thirty (30) days' notice in writing of any change to the format and shall specify the date from which it must be used.

9.3 The Supplier further agrees and acknowledges that it may not make any amendment to the current MI Reporting Template without the prior written approval of the Authority.

10. PAYMENT PLANNER

10.1 Except for TS Catalogue Item Charges, the Supplier shall ensure that the Payment Planner in the format set out in Annex E (*Payment Planner*) to Schedule 15 details all anticipated TS Charges.

10.2 The Supplier shall ensure that the information relating to the TS Charges contained in the Payment Planner is consistent with the TS Financial Model and is kept up to date on at least a monthly basis.

10.3 Not used.

10.4 The draft Payment Planner shall at all times be accompanied by sufficient information to enable the Authority to reasonably assess whether the TS Charges detailed therein are properly payable. Any such assessment by the Authority shall not be conclusive. The Supplier shall provide to the Authority any other documentation relating to the TS Charges reasonably required by the Authority from time to time to substantiate an invoice.

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 10.5 The Payment Planner shall be based on volume information which has been verified in accordance with the Transitional Services Description.
- 10.6 For the avoidance of doubt, the TS Charges appearing in the Payment Planner are TS Charges which are scheduled for payment in the month to which the Payment Planner relates, not the month in which the Transitional Services to which the TS Charges relate are performed. For example, if a Milestone Achievement Certificate has not been issued by the Authority by the time the draft Payment Planner is submitted, then such amounts should not be included under the current month's TS Charges in the Payment Planner. They should instead be deferred until the Milestone Achievement Certificate has been issued but should still be included in the Payment Planner (under a future month), so that the Authority retains visibility of when such payments are scheduled to be paid.
- 10.7 Not used.
- 10.8 The Supplier will attend a Payment Planner review meeting with the Authority as required under Schedule 15, where the proposed TS Charges in the Payment Planner will be reviewed, discussed, agreed, or disputed by the Authority. Any disputed or missing TS Charges which require clarification or where additional information is being sought or cannot be cleared by the time the final Payment Planner is submitted under Schedule 15 are to be deferred to the next payment month and recorded in the Payment Planner for consideration in the next Payment Planner review meeting. This allows for the un-disputed items to be paid.
- 10.9 Not used.
- 10.10 Not used.
- 10.11 Not used.
- 10.12 Not used.

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

APPENDIX A

CERTIFICATE OF TS COSTS

Certificate of TS Costs – Sample Report

For the Period of [insert date] (Start of Contract) through [insert date] (Start of Contract + 1 year)

Labour	£XXXX	
Labour Overhead	£XXXX	
Purchases	£XXXX	
Purchases Overhead	£XXXX	
Travel	£XXXX	
Other Value-Add	£XXXX	
General & Administrative	£XXXX	
Other Non-Value	£XXXX	
Total Cost	£XXXX	
Profit	<u>£XXXX</u>	
Total Price		£XXXX

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

APPENDIX B

MONTHLY TS SERVICE CHARGES

1. Subject to Paragraphs 3 to 7 inclusive, the Monthly TS Service Charges payable as at the Transitional Services Commencement Date shall be as shown in Table 1:

Table 1 - Monthly TS Service Charges

Service / Product	Corresponding requirements of Annex 2 (Transitional Services Description) to Schedule 34	Monthly Recurring Charges (MRC)
TS Gateway Test System	Paragraph 1.1.2.9 of Appendix B (TS Technical Requirements)	[REDACTED]
PSN WAN Services (Private VPN Service)	Paragraph 2.2.1(a) of Appendix B (TS Technical Requirements)	
Enterprise broadband	Paragraph 2.2.1(b)(i) of Appendix B (TS Technical Requirements)	
Mobile broadband	Paragraph 2.2.1(b)(ii) of Appendix B (TS Technical Requirements)	
DIA	Paragraph 2.3.1(a) of Appendix B (TS Technical Requirements)	
[REDACTED]	Paragraph 2.3.1(b) of Appendix B (TS Technical Requirements)	
Digital Prisons	Paragraph 2.3.2 of Appendix B (TS Technical Requirements)	
TS Gateway	Paragraph 2.4 of Appendix B (TS Technical Requirements)	
ITIL Service Management	Appendix A (TS Service Management Requirements)	

NOTE: The Monthly Recurring Charges (MRC) shown in the above table have been calculated on the basis set out within the [REDACTED]. In the event of changes to volumes, any resulting changes to the Monthly Recurring Charges will be agreed between the Parties.

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

2. The Monthly TS Service Charges within this Appendix B are subject to Indexation.
3. The Monthly TS Service Charges shall reduce over the TS Term. The Supplier shall cease to invoice the Authority for, and the Authority shall have no obligation to pay, the relevant proportion (as determined from the TS Financial Model) of Monthly TS Service Charges from the date of the event described in Table 2:

Table 2 - Reductions in Monthly TS Service Charges

Product (as defined in Table 1)	Event resulting in reduced monthly recurring charges
PSN WAN Services (Private VPN Service)	In respect of an Authority Site, the Authority issues a Site Transition Certificate.
Enterprise broadband	In respect of an Authority Site, the Authority issues a Site Transition Certificate.
Mobile broadband	In respect of an Authority Site, the Authority issues a Site Transition Certificate.
DIA	In respect of an Authority Site, the Authority issues a Site Transition Certificate.
[REDACTED]	In respect of a firewall Device, the Device is decommissioned.
Digital Prisons	In respect of an Authority Site, the Authority issues a Site Transition Certificate.
TS Gateway	Milestone M11 (Gateway Services Transition) Achievement.

4. **ITIL Service Management Charges**
 - 4.1. During the TS Term, the Supplier shall manage the allocation of Supplier Personnel in the following roles proportionally to the volume of Authority Sites in scope at that time of (i) the Transitional Services and (ii) Operational Services respectively:
 - Service manager
 - Principal service manager
 - Capacity and configuration manager
 - Business care incident manager
 - Technical customer authority

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- Customer solution architect
- PMO specialist
- Supply chain management
- Customer account security manager

- 4.2. The Supplier shall use all reasonable endeavours during the TS Term to identify and implement opportunities allowing for a reduction in the number of Supplier Personnel allocated to the delivery of the Transitional Services and, accordingly, a reduction in the ITIL Service Management Charges element of the Monthly TS Service Charges.
- 4.3. Table 3 sets out a non-exhaustive list of circumstances which the Parties anticipate will result in a reduction in the ITIL Service Management Charges, together with the Supplier Personnel roles which are likely to be impacted in those circumstances:

Table 3 - Circumstances for reducing ITIL Service Management Charges (non-exhaustive list)

Circumstances	Roles
Milestone M11 (Gateway Services Transition) Achieved	• Capacity Configuration Manager • Business Care Incident Manager • PMO Specialist
Reduced TS Service Availability Hours (implemented by Change to Paragraph 2.2 of Annex 3 (TS Service Levels))	Service Agents, including out-of-hours Service Agents
Site Transition Certificates issued for 50% of Authority Sites in scope of Transition	• Service Agents • Lead Advisors • Dedicated Technical Coord • Service Desk Team Leader • Change Manager • Problem Manager • Commercial Management MOJ

- 4.4. The Supplier shall also:
- 4.4.1. accept any Change Requests from the Authority requiring a reduction in the Supplier Personnel allocated to the Transitional Services; and
- 4.4.2. include in the Impact Assessment for any such Change Request the relevant reduction in the ITIL Service Management Charges element of the Monthly TS Service Charges, such reduction to be calculated by

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

revising the TS Financial Model in accordance with Schedule 19
(*Financial Reporting and Audit Rights*).

5. Following any month in which Site Transition Certificates have been issued, the Supplier shall provide a report on the allocation of Supplier Personnel in accordance with Paragraph 4.1, for the next Commercial Board meeting.
6. Subject to any revisions to such report reasonably required by the Commercial Board, the Supplier shall:
 - 6.1. provide a draft updated TS Financial Model to reflect changes to the allocation of Supplier Personnel; and simultaneously
 - 6.2. submit a Change Request to reduce the ITIL Service Management Charges element of the Monthly TS Service Charges accordingly.
7. Following agreement of the Change Request, the Supplier shall update the TS Financial Model and the Payment Planner to reflect the reduction in the Monthly TS Service Charges in accordance with the approach set out above.

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

APPENDIX C

TS PRODUCT AND SERVICE CATALOGUE

Note: As at the Effective Date, there are no products or services listed within the TS Product and Service Catalogue. Any additions to the TS Product and Service Catalogue will be made in accordance with Paragraph 3.7 of this Annex 15.

**Annex 15 (TS CHARGES AND INVOICING) to
Schedule 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

APPENDIX D

TS RATE CARD

TABLE 1: TS RATE CARD

The Rate Card applying to the Transitional Services shall be the same as the Rate Card in Schedule 15.

TABLE 2: UTILISATION DISCOUNT

Period of deployment	Utilisation Discount %
from 110 Working Days to 219 Working Days	[REDACTED]
from 220 Working Days to 439 Working Days	
More than 440 Working Days	

TABLE 3: VOLUME REBATE ON TS RATE CARD RELATED CHARGES

Value (£) invoiced in Contract Year		Rebate %
£500,000	£1,000,000	[REDACTED]
£1,000,001	£5,000,000	
£5,000,001+		

**ANNEX 16 (PAYMENTS ON TS TERMINATION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 16

PAYMENTS ON TS TERMINATION

**ANNEX 16 (PAYMENTS ON TS TERMINATION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

1. PURPOSE OF SCHEDULE

- 1.1 This Annex 16 (*Payments on TS Termination*) sets out the calculation of the TS Termination Payment that may be paid by the Authority to the Supplier pursuant to Paragraph 32.4 (*Payments by the Authority*) of this Schedule 34.

2. GENERAL PRINCIPLES

- 2.1 The Parties acknowledge that this Schedule 34 is intended to facilitate a planned phased cessation of the Transitional Services over the TS Term. The Supplier shall work with the Authority to mitigate or avoid the requirement for a TS Termination Payment to be made.
- 2.2 The Authority shall only be liable to pay a TS Termination Payment to the Supplier in the following circumstances:
- 2.2.1 if the Transitional Services are terminated by the Authority pursuant to Clause 31.1(a) (*Termination by the Authority*);
- 2.2.2 (subject to Paragraph 2.3 below) if any part of the Transitional Services are terminated by the Authority pursuant to Clause 31.1A (*Partial Termination for Convenience*);
- 2.2.3 if the Transitional Services are terminated by the Supplier pursuant to Clause 31.3(a) (*Termination by the Supplier*); or
- 2.2.4 if this Contract is terminated by the Supplier pursuant to Clause 34.4 (*Assignment and Novation*).
- 2.3 The Parties agree that the following will not amount to a Partial Termination for the purposes of this Schedule 34:
- 2.3.1 the cessation of Transitional Services at an Authority Site in accordance with the Implementation Plan; and
- 2.3.2 the closure of an Authority Site or a reduction in Transitional Services through business-as-usual activity,
- and for the avoidance of doubt, the Supplier shall not be entitled to receive any TS Termination Payment from the Authority in respect of such closure of an Authority Site or cessation or reduction in Transitional Services.
- 2.4 The amount of the TS Termination Payment payable by the Authority shall be determined in accordance with Paragraph 4 of this Annex 16.

**ANNEX 16 (PAYMENTS ON TS TERMINATION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

2.5 If the Transitional Services are terminated for any reason other than in the circumstances listed in Paragraph 2.2, no TS Termination Payment shall be due to the Supplier and the following paragraphs of this Annex 16 shall not be applicable:

2.5.1 Paragraph 4 (TS Termination Payments);

2.5.2 Paragraph 6 (Full and Final Settlement);

2.5.3 Paragraph 7 (Mitigation of TS Breakage Costs);

2.5.4 Paragraph 8 (Invoicing for the TS Payments on Termination);

2.5.5 Paragraph 9 (Set Off); and

2.5.6 Paragraph 10 (No Double Recovery).

2.6 Except as expressly set out in Paragraphs 32.4 and 32.5 (*Payments by the Authority*) of Schedule 34, this Annex 16, Schedule 25 (*Exit Management*) and Annex 25 (*TS Exit Management*), no other termination or compensation payments (including compensation for loss of profits) shall therefore be payable to the Supplier as a result of termination, Partial Termination, reduction in or cessation of any of the Transitional Services or expiry of the TS Term.

3. CHARGES TO SUPPORT EXIT MANAGEMENT

3.1 The Supplier shall perform the Termination Services relating to the Transitional Services in accordance with any Termination Assistance Notice issued by the Authority pursuant to Schedule 25 (*Exit Management*).

3.2 The Supplier shall charge for the TS Termination Services in accordance with Annex 25 (*TS Exit Management*) and Annex 15 (*TS Charges and Invoicing*).

4. TS TERMINATION PAYMENT

4.1 In the event that:

4.1.1 the Authority terminates the Transitional Services in the circumstances set out in Paragraph 2.2.1 above; or

4.1.2 the Authority terminates any part of the Transitional Services in the circumstances set out in Paragraph 2.2.2 above; or

4.1.3 the Supplier terminates the Transitional Services in the circumstances set out in Paragraph 2.2.3 above,

**ANNEX 16 (PAYMENTS ON TS TERMINATION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

then the Authority shall pay to the Supplier a sum ("**the TS Termination Payment**") equal to those costs which are:

- 4.1.4 reasonably and properly incurred by the Supplier directly as a result of the termination (or partial termination) and which would not have been incurred had the Transitional Services continued until expiry of the TS Term;
- 4.1.5 unavoidable (notwithstanding that the Supplier and any relevant Sub-Contractor has each used reasonable endeavours to mitigate those costs in accordance with Paragraph 7);
- 4.1.6 supported by disclosure of appropriate information identifying the costs incurred by the Supplier;
- 4.1.7 not capable of recovery; and
- 4.1.8 represent the Supplier's TS Breakage Costs and TS Unrecovered Costs, calculated in accordance with the principles set out in Appendix 1 (*Methodology for Calculating TS Termination Payment*).

4.2 [REDACTED]

4.3 Regardless of the notice period given for a termination for convenience, or whether the Transitional Services are terminated by the Supplier pursuant to Clause 31.3 (*Termination by the Supplier*), a termination charge shall be due from the Authority to the Supplier specifically where any TS Unrecovered Costs have been incurred in relation to on-going TS Service Requests and in accordance with any termination provisions specifically set out in ongoing Project Work Orders (including the deployment of TS Assets) that will not now be completed under this Schedule 34 due directly to the termination.

5. CHARGES FOR TS ASSETS AT TERMINATION

5.1 The Parties acknowledge that, as at the Effective Date:

- 5.1.1 all Exclusive Assets used in the provision of the Transitional Services are owned by the Authority; and
- 5.1.2 the Authority has granted the Supplier the right to use those Exclusive Assets for the TS Term solely for the purpose of providing the Transitional Services under this Schedule 34.

**ANNEX 16 (PAYMENTS ON TS TERMINATION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 5.2 In the event, during the TS Term, any new assets (in addition to the Exclusive Assets) are required for the delivery of the Transitional Services ("**New TS Assets**"), then unless specifically agreed otherwise by the Parties those New TS Assets will be purchased by the Supplier on behalf of the Authority.
- 5.3 Accordingly, the Parties agree that (unless agreed otherwise in accordance with the Change Control Procedure), the Supplier shall:
- 5.3.1 subject to Paragraph 5.3.2 in respect of Non-Exclusive Assets only, not be entitled to receive any payment in respect of TS Assets (including Exclusive Assets and/or New TS Assets) on or after the termination of the TS Termination Services (for whatever reason);
- 5.3.2 only where the Authority has exercised its option to purchase itself or for any Replacement Supplier to purchase any TS Asset which is a Non-Exclusive Asset in accordance with Paragraph 7.2(a) of Schedule 25 (*Exit Management*), be entitled to receive payment in respect of the relevant Non-Exclusive Asset, in such case the applicable payment will be equal to the Net Book Value of the relevant asset as reported by the Supplier in accordance with Annex 25 (*TS Exit Management*), except where the cost of the Non-Exclusive Asset has been partially or fully paid for through the TS Charges at the time of expiry or termination of the Transitional Services, in which case the Authority shall pay (either for itself or on behalf of the relevant Replacement Supplier) the Supplier the Net Book Value of the Non-Exclusive Asset less the amount already paid through the TS Charges; and
- 5.3.3 only where the Authority (or any Replacement Supplier) has exercised its option to use, rent or licence any Non-Exclusive Asset in accordance with Paragraph 7.2(b) of Schedule 25 (*Exit Management*), be entitled to receive payment in respect of the relevant Non-Exclusive Asset from the Authority (either for itself or on behalf of the relevant Replacement Supplier) in accordance with Paragraph 7.6 of Annex 25 (*TS Exit Management*).

6. FULL AND FINAL SETTLEMENT

- 6.1 This Paragraph 6.1 is subject to Paragraph 6.2. Any TS Termination Payment paid in accordance with this Annex 16 (*Payments on TS Termination*) shall be in full and final settlement of any claim, demand and/or proceedings of the Supplier in relation to:

**ANNEX 16 (PAYMENTS ON TS TERMINATION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 6.1.1 termination of this Contract by the Authority pursuant to Clause 31.1(a) or Clause 31.1(d) (*Termination by the Authority*);
- 6.1.2 termination of any part of the Transitional Services by the Authority pursuant to Clause 31.1A (*Partial Termination for Convenience*); and
- 6.1.3 termination of this Contract by the Supplier pursuant to Clause 31.3(a) or Clause 31.3(c) (*Termination by the Supplier*) or Clause 34.4.

Accordingly, the Supplier shall be excluded from all other rights and remedies it would otherwise have been entitled to in respect of any such termination. For the avoidance of doubt, this Paragraph 6.1 shall not affect or prejudice any claim or demand that either Party may have against the other under the indemnities in Schedule 28 (*Staff Transfers*), any indemnities set out in this Schedule 34 and any payments due to the Supplier for TS Termination Services provided during any TS Termination Assistance Period pursuant to Schedule 25 (*Exit Management*).

- 6.2 Termination of the Transitional Services shall not affect or prejudice any claim or demand that either Party may have against the other under or in connection with this Contract arising before, on or (for claims or demands under provisions that expressly survive the termination or expiry of the Transitional Services) after the date of termination that is not in respect of any such termination, including claims for recovery of TS Charges properly due for payment.

7. MITIGATION OF TS BREAKAGE COSTS AND TS UNRECOVERED COSTS

- 7.1 The Supplier shall take all reasonable steps to minimise and mitigate TS Breakage Costs and TS Unrecovered Costs incurred as a result of termination of all or part of the Transitional Services by:
 - 7.1.1 the appropriation of TS Assets, employees and resources for other purposes. If such TS Assets, employees and resources can be used for other purposes then there shall be an equitable reduction in the TS Termination Payment payable by the Authority to the Supplier; and
 - 7.1.2 in relation to contracts entered into with third parties, termination by the Supplier of those contracts at the earliest possible date without breach or where contractually permitted, and, where required by the Authority, assigning such contracts to the Authority or a third party acting on behalf of the Authority subject to Paragraph 2 of Annex 25 (*TS Exit Management*).

**ANNEX 16 (PAYMENTS ON TS TERMINATION) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

8. INVOICING FOR THE PAYMENTS ON TS TERMINATION

All sums due under this Annex 16 (*Payments on TS Termination*) shall be payable by the Authority to the Supplier in accordance with the invoicing and payment terms set out in Annex 15 (*TS Charging and Invoicing*).

9. SET OFF

For the avoidance of doubt, the Authority shall be entitled to set off any outstanding liabilities of the Supplier under this Schedule 34 against any amount it pays in TS Termination Payments pursuant to this Annex 16 (*Payments on TS Termination*) or Clause 32.4 or Paragraph 32.2 (*Payments by the Authority*) of Schedule 34 and in accordance with its rights set out in this Contract.

10. NO DOUBLE RECOVERY

- 10.1 If any payment pursuant to this Annex 16 relates to or arises in relation from (in whole or in part) any TS Asset then to the extent that the Authority makes any payments pursuant to Schedule 25 (*Exit Management*) or Annex 25 (*TS Exit Management*) in respect of such TS Assets then such amounts shall be deducted from the amount of compensation payable pursuant to this Annex 16.
- 10.2 The value of the TS Termination Payment shall be reduced or extinguished to the extent that the Supplier has already received the TS Charges or the financial benefit of any other remedy given under this Contract so that there is no double counting in calculating the relevant payment.

ANNEX 16 (PAYMENTS ON TS TERMINATION) to SCHEDULE 34

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

APPENDIX 1

Methodology for Calculating TS Termination Payment

The following components shall be considered when calculating the costs to be recovered by the Supplier in the TS Termination Payment:

Service Components/ Assets attracting TS Termination Payments	Circumstances in which TS Termination Payments apply (e.g. Minimum notice period)	Value/Method of Calculation of TS Termination Payments (e.g. contract breakage costs; unrecovered costs)	Steps to be taken by Authority or Supplier to mitigate/avoid TS Termination Payments
Circuits	[REDACTED]	[REDACTED]	[REDACTED]
Gateway Licences	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Gateway Maintenance	[REDACTED]	[REDACTED]	[REDACTED]

ANNEX 16 (PAYMENTS ON TS TERMINATION) to SCHEDULE 34

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

Service Components/ Assets attracting TS Termination Payments	Circumstances in which TS Termination Payments apply (e.g. Minimum notice period)	Value/Method of Calculation of TS Termination Payments (e.g. contract breakage costs; unrecovered costs)	Steps to be taken by Authority or Supplier to mitigate/avoid TS Termination Payments
Broadband	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

ANNEX 25 (TS EXIT MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 25

TS EXIT MANAGEMENT

ANNEX 25 (TS EXIT MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

1. INTRODUCTION

1.1 This Annex comprises the following elements:

1.1.1 **Paragraph 1A of this Annex 25:** sets out obligations relating to the planned transfer and exit from the Transitional Services on an Authority Site by Authority Site basis as envisaged under this Schedule 34 and the Implementation Plan; and

1.1.2 **Paragraphs 2 to 12 of this Annex 25:** sets out obligations relating to an unplanned exit from the Transitional Services (for example, following the termination of all or part of the Transitional Services).

1A PLANNED EXIT FROM THE TRANSITIONAL SERVICES

1A.1 The Supplier acknowledges that this Schedule 34 is intended to facilitate the smooth and flexible exit from the Transitional Services during the TS Term on an Authority Site by Authority Site basis in accordance with the Implementation Plan.

1A.2 The Supplier shall work collaboratively with the Authority to manage effectively and efficiently the planned exit and/or service transfer arrangements of the Transitional Services in accordance with the Implementation Plan.

1A.3 The Supplier acknowledges its obligation under Paragraph 14 (*Issue of a Site Transition Certificate*) of Schedule 14 (*Testing Procedures*) to provide evidence to the Authority where the Supplier has completed all applicable Implementation Services for the transition of an Authority Site into Operational Service. The Supplier shall in addition in relation to each TS Service Line:

1A.3.1 provide to the Authority evidence that the transition of the TS Service Line has been completed in accordance with the Implementation Plan, Schedule 13 (*Implementation*) and Schedule 2, Annex C (*Transition Requirements*) and to confirm to the Authority that the provision of that TS Service Line has ceased); and

1A.3.2 provide any additional information or assistance reasonably requested by the Authority in order to confirm that the transition of that TS Service Line has been completed.

2. OBLIGATIONS DURING THE TS TERM TO FACILITATE EXIT

2.1 Paragraph 2 (*Obligations during the Term to Facilitate Exit*) of Schedule 25 (*Exit Management*) shall apply.

2.2 During the TS Term the Supplier shall (in addition to the obligations set out in

ANNEX 25 (TS EXIT MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Paragraph 2.1 of Schedule 25 (*Exit Management*):

- 2.2.1 maintain a register (the “**TS Register**”) of all Authority Data relating to or arising from the Transitional Services contained in any applicable System Management Tools as well as any Databases and, where the Transitional Supplier is holding any such Authority Data on its own systems and providing updates to the System Management Tools, the Supplier shall maintain a register of all such Authority Data contained in its own systems. The Supplier shall maintain the TS Register in such format as is agreed in writing between the Parties and shall update the TS Register from time to time and in particular if TS Assets, Sub-contracts or other relevant agreements are added to or removed from the Transitional Services;
- 2.2.2 include in the configuration management database (maintained pursuant to Paragraph 2.1(b) of Schedule 25) clear and unequivocal statements in relation to the ownership of TS Assets, including IPRs;
- 2.2.3 create and maintain, in an electronic form, user data including all active users, e-mail addresses, location and contact details (such as e-mail addresses, locations and contact details as may be advised to the Supplier by the Authority), site and software licensing information.
- 2.3 The Supplier shall (unless otherwise agreed by the Authority in writing) procure that all Sub-contracts and other agreements with third parties, in each case that exclusively relate to the Transitional Services and which are necessary to enable the Authority and/or any Replacement Supplier(s) to perform the Transitional Services (in accordance with this Schedule 34) shall be assignable and/or capable of novation at the request of the Authority to the Authority (and/or its nominee) and/or any Replacement Supplier(s) upon the Supplier ceasing to provide the Transitional Services (or part of them) without restriction (including any need to obtain any approval) or payment by the Authority.
- 2.4 Where the Supplier is unable to procure that any Sub-contract or other agreement referred to in Paragraph 3.3 above which the Supplier proposes to enter into after the Effective Date is assignable and/or capable of novation to the Authority (and/or its nominee) and/or any Replacement Supplier(s) without restriction or payment, the Supplier shall promptly notify the Authority in writing of this and the Parties shall (acting reasonably and without undue delay) discuss the appropriate action to be taken which, where the Authority so directs, may include the Supplier seeking an alternative Sub-contractor, to be agreed in writing with the Authority.
- 2.5 The Supplier will ensure that any requests made by the Authority for the

ANNEX 25 (TS EXIT MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

provision of Authority Data or the TS Register are met in accordance with the provisions set out in Clause 18 (*Authority Data and Security Requirements*).

3. OBLIGATIONS TO ASSIST ON RE-TENDERING OF TRANSITIONAL SERVICES

3.1 Paragraph 3 (*Obligations to Assist on Re-Tendering of Services*) of Schedule 25 (*Exit Management*) shall apply provided that:

3.1.1 Paragraph 3.1(b) shall be deleted and replaced with the following:

“A copy of the Registers, including the TS Register, updated by the Supplier up to the date of delivery of Registers; including make, model and asset number (and any unrecovered capital costs of such assets) and details of their condition and physical location;”

3.1.2 The following shall be added as a new paragraph 3.1(h):

“(h) details of and information relating to the use and ownership of the TS Assets (including technical specifications) to the extent not set out in the Registers (including the TS Register);”

3.2 In the event that the Supplier fails to meet its obligations under Paragraph 3.1 of Schedule 25 (*Exit Management*) and without prejudice to any other rights or remedies arising as a result of such failure, the Authority, potential Replacement Supplier(s) or any advisors appointed by the Authority and subject to reasonable notice shall be granted unfettered access to the Authority Data and shall be entitled to gather any such Authority Data as may reasonably be required to meet the obligations set out in Paragraph 3.1 of Schedule 25 (*Exit Management*). Any additional costs incurred by the Authority and/or Replacement Supplier(s), to the extent arising from the Supplier's failure to comply with its obligations set out in Paragraph 3.1 of Schedule 25 (*Exit Management*), shall be recoverable by the Authority from the Supplier.

4. OBLIGATION TO ENTER INTO AN ETHICAL WALL AGREEMENT ON RE-TENDERING OF TRANSITIONAL SERVICES

4.1 Paragraph 4 (*Obligation to Enter into an Ethical Wall Agreement on Re-Tendering of Services*) of Schedule 25 (*Exit Management*) shall apply.

5. EXIT PLAN

5.1 Paragraph 5 (*Exit Plan*) of Schedule 25 (*Exit Management*) shall apply provided that, in Paragraph 5.3(j), any charges for Termination Services relating to the Transitional Services shall be calculated in accordance with the day rates and charging methodology set out in Annex 15 (*TS Charges and Invoicing*) and

ANNEX 25 (TS EXIT MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

having regard to the principles set out in Appendix 1 (*Principles for Determining Exit Charges, Costs and Expenses in Relation to Termination Services in Connection with the Transitional Services*) to this Annex 25.

6. TERMINATION SERVICES

6.1 Paragraph 6 (*Termination Services*) of Schedule 25 (*Exit Management*) shall apply, provided that Paragraph 6.7(b) shall be amended to read:

(b) “provide the Authority and/or the Replacement Supplier with a complete and uncorrupted version of the Authority Data in electronic form (or such other format as reasonably required by the Authority) together with an up-to-date TS Service Operations Manual;”

6.2 Paragraph 1.4(a) of Annex 1 (*Scope of the Termination Services*) to Schedule 25 (*Exit Management*) shall be amended to read as follows:

(a) “copies of up-to-date procedures and operations manuals, including a copy of the up-to-date TS Service Operations Manual;”

6.3 The Supplier acknowledges that the Transitional Services may be terminated in whole or in part and that, where they are terminated in part, Termination Services shall be needed in respect of each termination (however arising).

7. TS ASSETS, SUB-CONTRACTS AND SOFTWARE

7.1 Paragraph 7 (*Assets, Sub-Contracts and Software*) of Schedule 25 (*Exit Management*) shall apply except as provided for in this Paragraph 7.

7.2 Paragraph 7.1 (*Assets, Sub-Contracts and Software*) of Schedule 25 (*Exit Management*) shall be replaced with the following:

“During the TS Term and following termination (however arising) or Partial Termination of the Transitional Services (or any relevant part) and during any Termination Assistance Period, the Supplier shall not, without the Authority's Approval:

7.2.1 terminate, enter into or vary any Sub-contract relating to or required for the provision of the Transitional Services;

7.2.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing TS Assets or acquire any new TS Assets; or

7.2.3 terminate, enter into or vary any licence for software in connection with the Transitional Services.”

ANNEX 25 (TS EXIT MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Contract for the provision of WAN Services

Security Classification (Official)

Contract reference: [REDACTED]

7.3 Paragraph 7.2 of Schedule 25 (*Exit Management*) shall apply provided that, for the purposes of Paragraph 7.2(a), the definition of Transferring Assets shall include any TS Assets which the Authority requires to be transferred to the Authority and/or any Replacement Supplier(s).

7.4 Access to TS Assets may be required by the Authority before the date on which the Transitional Services will exit and/or transfer in accordance with the Exit Plan in order to continue to deliver the Transitional Services or business as usual and consent to this shall not be unreasonably withheld or delayed.

7.5 In relation to any TS Assets forming part of the Transferring Assets, the following shall apply in place of Paragraphs 7.3 and 7.4 of Schedule 25 (*Exit Management*):

“With effect from the expiry of the Termination Assistance Period, the Supplier shall assign to the Authority (and/or any nominated Replacement Supplier(s)), free from all liens, charges, options, encumbrances and third party rights, title to and all rights and interests in those TS Assets identified by the Authority pursuant to Paragraph 7.27.3 of Schedule 25 (Exit Management) which constitute Exclusive Assets or New TS Assets. Except for any TS Assets which are Non-Exclusive Assets, the Supplier shall not be entitled to receive any payment in respect of such TS Assets and Paragraph 5.3 of Annex 16 (Payments on TS Termination) shall apply”.

7.6 The following provisions shall apply in place of Paragraph 7.5 of Schedule 25 (*Exit Management*):

“The Supplier shall:

- 7.5.1 not unreasonably withhold its consent to sell to the Authority and/or any Replacement Supplier(s) any TS Assets which constitute Non-Exclusive Assets and are identified as Transferring Assets in the Authority’s notice provided pursuant to Paragraph 7.2(a) of Schedule 25 (Exit Management). The Supplier shall only be entitled to be paid for such Non-Exclusive Assets as set out in Paragraph 5.3.2 of Annex 16 (Payments on TS Termination); or*
- 7.5.2 procure for the Authority and/or any Replacement Supplier(s) the continued use, rental or licensing (as appropriate) of any TS Assets which constitute Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets notified by the Authority pursuant to Paragraph 7.2(b) of Schedule 25 (Exit Management) in each case for such period of time and on such commercial and other terms as may be agreed in writing between the Parties, acting fairly and*

ANNEX 25 (TS EXIT MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

reasonably and taking account of any TS Termination Payment in relation to those TS Assets. Where the Authority and/or any Replacement Supplier(s) are to have such use of the relevant TS Asset, this shall be at a fair market price or rent for the life of the TS Asset. For a multiple use TS Asset this shall be for up to two (2) years (or such other period as the Parties agree in writing) on the same capacity basis as a fair market rent."

7.7 Paragraphs 7.6 to 7.9 of Schedule 25 (*Exit Management*) shall apply.

7.8 Once they are no longer needed to provide the Transitional Services or the Termination Services, the Supplier shall disconnect and remove from the Authority Premises any of its TS Assets which are not acquired by the Authority pursuant to Paragraph 7 of Schedule 25 (*Exit Management*) and/or this Paragraph 7.

8. SUPPLIER PERSONNEL

8.1 Paragraph 8 (*Supplier Personnel*) of Schedule 25 (*Exit Management*) shall apply, provided that the obligation in Paragraph 8.3 to give access to the Supplier's personnel shall also apply during the TS Term.

9. CHARGES

9.1 Paragraph 9 (*Charges*) of Schedule 25 (*Exit Management*) shall apply.

10. APPORTIONMENTS

10.1 Paragraph 10 (*Apportionments*) of Schedule 25 (*Exit Management*) shall apply.

11. PARTIAL TERMINATION FOR CONVENIENCE OF TRANSITIONAL SERVICES

11.1 Paragraph 11 (*Partial Termination for Convenience of Transitional Services*) of Schedule 25 (*Exit Management*) shall apply. .

12. IN-PROGRESS TS PROJECTS

12.1 Following the commencement of any Termination Assistance Period, the Supplier shall review all outstanding offers to provide additional Transitional Services initiated pursuant to the Change Control Procedure and identify the current status, benefits, costs and risks involved for each. The Authority and the Supplier shall review each such outstanding offer and (subject to the other provisions of this Annex 25) agree for each one whether:

12.1.1 the offer shall be accepted by the Authority; or

ANNEX 25 (TS EXIT MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential

Security Classification (Official)

Contract for the provision of WAN Services

Contract reference: [REDACTED]

- 12.1.2 further work shall be undertaken by the Supplier in respect of the offer up to an agreed Milestone Date or up to an agreed checkpoint in respect of such offer.
- 12.2 Alternatively, the Authority may decide that no further work shall be undertaken by the Supplier in respect of the offer, in which event the Supplier shall document the status of the offer and recommend a reasonable exit and hand-over strategy for that offer.

ANNEX 25 (TS EXIT MANAGEMENT) to Schedule 34 (Transitional Services)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

APPENDIX 1

Principles for Determining Exit Charges, Costs and Expenses in Relation to TS Termination Services in Connection with Transitional Services

1. Save where stated otherwise in this Annex 25 (*TS Exit Management*), the Supplier shall not be entitled to claim any additional charges, costs or expenses from the Authority, in relation to the Termination Services in respect of:
 - a) providing information, documentation and reports for exit related purposes which are, or should be, available under the terms of this Schedule 34;
 - b) providing information, documentation and reports for exit related purposes which can be produced without material incremental cost using information already held by the Supplier;
 - c) exit related activities and support which can reasonably be provided using existing resources, including staff who are already providing the Transitional Services, to perform such exit support and assistance;
 - d) costs and expenses incurred by the Supplier as a result of its Defaults or delays in performing the Termination Services save where such Defaults or delays are caused by the Authority and/or the Replacement Supplier(s);
 - e) providing reasonable access to Supplier's premises for exit related purposes;
 - f) any TS Charges, costs or expenses which the Supplier has recovered, or reasonably expects to recover, pursuant to any other provision of this Contract, including but not limited to any payments received:
 - (i) pursuant to Paragraphs 32.2 and 32.3 (*Payments by the Authority*) of Schedule 34;
 - (ii) for delivery of any part of or all of the Transitional Services during the TS Term; and
 - (iii) for performance of any of the Supplier's obligations as set out in any clauses, provisions or Annexes of this Schedule 34 (other than this Annex).
2. The Supplier shall use all reasonable endeavours to mitigate any costs and expenses incurred in relation to exit of the Transitional Services and/or the performance of the Termination Services in connection with the Transitional Services.

ANNEX 29 (TS KEY PERSONNEL) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 29

TS KEY PERSONNEL

ANNEX 29 (TS KEY PERSONNEL) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Annex 29 (TS Key Personnel)

1. This Annex lists the key roles (“**TS Key Roles**”) and names of the persons who the Supplier appoint to fill those TS Key Roles at the Effective Date (“**TS Key Personnel**”).

Key Role	Name of Key Personnel	Responsibilities	Phase of the Transitional Services during which they will be a member of TS Key Personnel

[REDACTED]			

**ANNEX 32 (TS INTELLECTUAL PROPERTY RIGHTS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

ANNEX 32

TS INTELLECTUAL PROPERTY RIGHTS

**ANNEX 32 (TS INTELLECTUAL PROPERTY RIGHTS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Annex 32 (*TS Intellectual Property Rights*)**1 TS INTELLECTUAL PROPERTY RIGHTS**

- 1.1 In respect of the Transitional Services only, except as expressly set out in this Schedule 34:
- (a) the Authority shall not acquire any right, title or interest in or to the Intellectual Property Rights of the Supplier or its licensors, namely:
 - (i) the TS Supplier Software;
 - (ii) the TS Third Party Software;
 - (iii) the TS Third Party IPRs; and
 - (iv) the TS Background IPRs;
 - (b) the Supplier shall not acquire any right, title or interest in or to the Intellectual Property Rights of the Authority or its licensors, including:
 - (i) the Authority Software;
 - (ii) the Authority Data; and
 - (iii) the Authority Background IPRs;
 - (c) TS Specially Written Software and TS Project Specific IPRs shall be the property of the Supplier.
- 1.2 Where either Party acquires, by operation of law, title to Intellectual Property Rights that is inconsistent with the allocation of title set out in Paragraph 1.1, it shall assign (or procure the assignment of) in writing such Intellectual Property Rights as it has acquired to the other Party on the request of the other Party (whenever made).
- 1.3 Neither Party shall have any right to use any of the other Party's names, logos or trade marks on any of its products or services without the other Party's prior written consent.
- 1.4 Unless otherwise agreed in writing, the Parties shall record all TS Specially Written Software and TS Project Specific IPRs in Appendix 1 to this Annex **Annex 32 (*TS Intellectual Property Rights*)** and shall keep Appendix 1 updated during the Term.

**ANNEX 32 (TS INTELLECTUAL PROPERTY RIGHTS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

2 TRANSFER AND LICENCES GRANTED BY THE SUPPLIER**TS Specially Written Software and TS Project Specific IPRs**

- 2.1 Subject to Paragraphs 2.3 and 2.18 (*TS Patents*) the Authority hereby agrees to transfer to the Supplier, or shall procure the transfer to the Supplier of, all rights (subject to Paragraph 1.1(a) (*TS Intellectual Property Rights*)) not already resting with the Supplier in the TS Specially Written Software and the TS Project Specific IPRs including (without limitation):
- (a) the TS Documentation, Source Code and the Object Code of the TS Specially Written Software; and
 - (b) all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the TS Specially Written Software (together the "**TS Software Supporting Materials**").
- 2.2 The Authority shall execute, or procure the execution of, all such assignments as are required to ensure that any rights in the TS Specially Written Software and TS Project Specific IPRs are properly transferred to the Supplier.
- 2.3 If within three years of its creation, any Intellectual Property in the TS Specially Written Software and/or the TS Project Specific IPRs has not been commercially exploited by the Supplier, and the Supplier is not using its best endeavours to do so, the Supplier shall on written request by the Authority promptly assign the Intellectual Property Rights in the TS Specially Written Software and/or the TS Project Specific IPRs to the Authority. Each party shall bear its own costs in such assignment. This Paragraph 2.3 shall not apply in respect of:
- (a) TS LLDs; or
 - (b) items or materials created by the Supplier for use in the provision of WAN services, or other services substantially similar to the Transitional Services, generally to customers of the Supplier.

TS Supplier Software, TS Specially Written Software, TS Project Specific IPRs, and TS Background IPRs

- 2.4 The Supplier shall not use any TS Non-COTS Software or TS Non-COTS Background IPRs in the provision of the Transitional Services unless it is detailed in Annex 12 (*TS Software*) to Schedule 34; or sent to the Enterprise Architecture Board for review and approval granted by the Authority. Prior to the use of any TS Non-COTS Software or TS Non-COTS Background IPR in the provision of the Transitional Services, the Supplier shall notify the Authority in writing giving details of any Know-How, trade secrets or Confidential Information contained in the TS Non-COTS Software or TS Non-COTS Background IPR and whether there are any restrictions on its use

ANNEX 32 (TS INTELLECTUAL PROPERTY RIGHTS) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

which are inconsistent with any of the rights and licences granted to the Authority and/or the Service Recipients under this Annex 32.

2.5 The Supplier hereby grants to the Authority and the Service Recipients:

- (a) subject to the provisions of Paragraph 2.18 (*TS Patents*), perpetual, royalty-free and non-exclusive licences to use (including but not limited to the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display)):
 - (i) the TS Non-COTS Software for which the Supplier delivers a copy to the Authority for any purpose relating to the Transitional Services (or substantially equivalent services whether in whole or in part) or for any purpose relating to the exercise of the Authority's (or any other Central Government Body's) business or function; and
 - (ii) subject to the provisions in Paragraph 2.5A, the TS Non-COTS Background IPRs, the TS Specially Written Software and the TS Project Specific IPRs for any purpose relating to the Transitional Services (or substantially equivalent services whether in whole or in part) or for any purpose relating to the exercise of the Authority's (or any other Central Government Body's) business or function;
- (b) a licence to use the TS COTS Software for which the Supplier delivers a copy to the Authority and TS COTS Background IPRs on the licence terms identified in a letter in or substantially in the form set out in Appendix 1 to Annex 12 (*TS Software*) and signed by or on behalf of the Parties on or before the Effective Date provided always that the Authority shall remain entitled to sub-license and to assign and novate the TS COTS Software and TS COTS Background IPRs on equivalent terms to those set out in Paragraphs 2.8 (*Right to sub-licence*) and 2.9 (*Right to assign/novate sub-licences*) in relation to the TS Non-COTS Software and TS Non-COTS Background IPRs; and
- (c) subject to the provisions in Paragraph 2.5A, a perpetual royalty-free non-exclusive licence to use without limitation any Know-How, trade secrets or Confidential Information contained within the TS Specially Written Software or the TS Project Specific IPRs.

The Authority and the Service Recipients are only permitted to use the software and IPRs licensed under this Paragraph 2.5 to the extent set out in the relevant sub-paragraph of this Paragraph 2.5, and use of such software and/or IPRs by the Authority or a Service Recipient contrary to the relevant sub-paragraph of this Paragraph 2.5 shall constitute a breach of that sub-paragraph.

**ANNEX 32 (TS INTELLECTUAL PROPERTY RIGHTS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 2.5A The TS Hardened Builds shall be licensed in accordance Paragraph 2.5(a)(ii) provided that:
- (a) no access or licence shall be granted in respect of the management layer in the Supplier's network operations centre, and
 - (b) the Supplier shall reconfigure the management configuration in the TS Hardened Builds that is used in the TS Gateway to ensure any Replacement Supplier has access to and is able to deliver the TS Gateway under this Contract after the Transitional Services terminate or expire.
- 2.6 At any time during the TS Term the Supplier may terminate the licence granted in respect of the TS Non-COTS Software under Paragraph 2.5(a)(i) or in respect of the TS Non-COTS Background IPRs under Paragraph 2.5(a)(ii) by giving thirty (30) days' notice in writing (or such other period as agreed by the Parties) if the Authority or any person to whom the Authority grants a sub-licence pursuant to Paragraph 2.8 (*Right to sub-license*), commits any material breach or material infringement of the terms of Paragraph 2.5(a)(i) or 2.5(a)(ii) or 2.8(a)(ii) which, if capable of remedy, is not remedied within 20 Working Days after the Supplier gives the Authority written notice specifying the breach and requiring its remedy.
- 2.7 In the event the licence of the TS Non-COTS Software or the TS Non-COTS Background IPRs is terminated pursuant to Paragraph 2.6, the Authority shall:
- (a) immediately cease all use of the TS Non-COTS Software or the TS Non-COTS Background IPRs (as the case may be);
 - (b) at the discretion of the Supplier, return or destroy documents and other tangible materials to the extent that they contain any of the TS Non-COTS Software and/or the TS Non-COTS Background IPRs, provided that if the Supplier has not made an election within 6 months of the termination of the licence, the Authority may destroy the documents and other tangible materials that contain any of the TS Non-COTS Software and/or the TS Non-COTS Background IPRs (as the case may be); and
 - (c) ensure, so far as reasonably practicable, that any TS Non-COTS Software and/or TS Non-COTS Background IPRs that are held in electronic, digital or other machine-readable form ceases to be readily accessible (other than by the information technology staff of the Authority or a Service Recipient) from any computer, word processor, voicemail system or any other device containing such TS Non-COTS Software and/or TS Non-COTS Background IPRs.

**ANNEX 32 (TS INTELLECTUAL PROPERTY RIGHTS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Right to sub-license

2.8 Subject to Paragraph 2.18 (*TS Patents*) the Authority may sub-license:

- (a) the rights granted under Paragraph 2.5(a) (*TS Supplier Software, TS Specially Written Software, TS Project Specific IPRs and TS Background IPRs*) to a third party (including for the avoidance of doubt, any Replacement Supplier) provided that:
 - (i) the sub-licence is on terms no broader than those granted to the Authority;
 - (ii) the sub-licence authorises the third party to use the rights licensed in Paragraph 2.5(a) (*TS Software, TS Specially Written Software, TS Project Specific IPRs and TS Background IPRs*) only for purposes relating to the Transitional Services (or substantially equivalent services) or for any purpose relating to the exercise of the Authority's (or any other Central Government Body's) business or function; and
 - (iii) the sub-licensee shall have executed a confidentiality undertaking in favour of the Supplier in or substantially in the form set out in Appendix 2 to Annex 12 (*TS Software*) to this Schedule 34 and
- (b) the rights granted under Paragraph 2.5(a) (*TS Supplier Software, TS Specially Written Software, TS Project Specific IPRs and TS Background IPRs*) to any Approved Sub-Licensee to the extent necessary to use and/or obtain the benefit of the TS Specially Written Software and/or the TS Project Specific IPRs provided that:
 - (i) the sub-licence is on terms no broader than those granted to the Authority; and
 - (ii) the Supplier has received a confidentiality undertaking in its favour in or substantially in the form set out in Appendix 2 to Annex 12 (*TS Software*) to this Schedule 34 duly executed by the Approved Sub-Licensee.

Right to assign/novate licences

2.9 The Authority and the Service Recipients may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to Paragraph 2.5(a) (*TS Supplier Software, TS Specially Written Software, TS Project Specific IPRs and TS Background IPRs*) to:

- (a) a Central Government Body; or
- (b) to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had

**ANNEX 32 (TS INTELLECTUAL PROPERTY RIGHTS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

been performed and/or carried on by the Authority or any Service Recipient.

- 2.10 Any change in the legal status of the Authority or a Service Recipient which means that it ceases to be a Central Government Body shall not affect the validity of any licence granted in Paragraph 2.5 (*TS Supplier Software, TS Specially Written Software, TS Project Specific IPRs and TS Background IPRs*). If the Authority or a Service Recipient ceases to be a Central Government Body, the successor body to the Authority or Service Recipient shall still be entitled to the benefit of the licence granted in Paragraph 2.4 (*TS Supplier Software, TS Specially Written Software, TS Project Specific IPRs and TS Background IPRs*).
- 2.11 If a licence granted in Paragraph 2.5 (*TS Software, TS Specially Written Software, TS Project Specific IPRs and TS Background IPRs*) is novated under Paragraph 2.9 (*Right to assign/novate licences*) or there is a change of the Authority's or Service Recipient's status pursuant to Paragraph 2.10, the rights acquired on that novation or change of status shall not extend beyond those previously enjoyed by the Authority and/or Service Recipient.

TS Third Party Software and TS Third Party IPRs

- 2.12 The Supplier shall not use in the provision of the Transitional Services (including in any TS Specially Written Software or in the software element of TS Project Specific IPRs) any Third Party Non-COTS Software or Third Party Non-COTS IPRs unless detailed in Annex 12 (*TS Software*) or approval is granted by the Authority following a review by the Enterprise Architecture Board and has in each case either:
- (a) first procured that the owner or an authorised licensor of the relevant Third Party Non-COTS IPRs or Third Party Non-COTS Software (as the case may be) has granted a direct licence to the the Authority and the Service Recipients on a royalty-free basis to the Authority and the Service Recipients and on terms no less favourable to the Authority and the Service Recipients than those set out in Paragraphs 2.5(a) and 2.6 (*TS Supplier Software, TS Specially Written Software, TS Project Specific IPRs and TS Supplier Background IPRs*) and Paragraph 2.9 (*Right to assign/novate licences*); or
 - (b) complied with the provisions of Paragraph 2.18.
- 2.13 If the Supplier cannot obtain for the Authority and Service Recipients a licence in respect of any Third Party Non-COTS Software and/or Third Party Non-COTS IPRs in accordance with the licence terms set out in Paragraph 2.12(a), the Supplier shall:
- (a) notify the Authority in writing giving details of what licence terms can be obtained from the relevant third party and whether there are

ANNEX 32 (TS INTELLECTUAL PROPERTY RIGHTS) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- alternative software providers which the Supplier could seek to use;
and
- (b) use the relevant Third Party Non-COTS Software and/or Third Party Non-COTS IPRs only if the Authority has first approved in writing either:
 - (i) the terms of the licence from the relevant third party; or
 - (ii) use without a licence, with reference to the acts authorised and the specific IPR involved. In spite of any other provisions of this Schedule 34 and for the avoidance of doubt, award of this Contract by the Authority and the ordering of any Deliverable under it does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977 Section 12 of the Registered Designs Act 1949 or Sections 240 – 243 of the Copyright, Designs and Patents Act 1988.

2.14 The Supplier shall:

- (a) notify the Authority in writing of all Third Party COTS Software and Third Party COTS IPRs that it uses and the terms on which it uses them; and
- (b) unless instructed otherwise in writing by the Authority in any case within 15 Working Days of notification pursuant to Paragraph 2.14(a) use all reasonable endeavours to procure in each case that the owner or an authorised licensor of the relevant Third Party COTS Software and Third Party COTS IPRs grants a direct licence to the Authority and the Service Recipients on terms no less favourable (including as to indemnification against IPRs Claims) than those on which such software is usually made commercially available by the relevant third party.

- 2.15 Should the Supplier become aware at any time, including after termination, that the TS Specially Written Software and/or the TS Project Specific IPRs contain any Intellectual Property Rights for which the Authority and the Service Recipients do not have a suitable licence, then the Supplier must notify the Authority within eight (8) days of what those rights are and which parts of the TS Specially Written Software and the TS Project Specific IPRs they are found in.

Termination and Replacement Suppliers

- 2.16 For the avoidance of doubt, the expiry of the TS Term or termination of the Transitional Services shall not of itself result in any termination of any of the licences granted by the Supplier or relevant third party pursuant to or as contemplated by this Paragraph 2.

ANNEX 32 (TS INTELLECTUAL PROPERTY RIGHTS) to SCHEDULE 34 (TRANSITIONAL SERVICES)

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

2.17 The Supplier shall, if requested by the Authority in accordance with Annex 25 (*TS Exit Management*) to this Schedule 34 and at the Supplier's cost:

- (a) grant (or procure the grant) to any Replacement Supplier of:
 - (i) a licence to use any TS Non-COTS Software, TS Non-COTS Background IPRs, Third Party Non-COTS IPRs, TS Specially Written Software, TS Project Specific IPRs and/or Third Party Non-COTS Software on a royalty-free basis to the Replacement Supplier and on terms no less favourable than those granted to the Authority and the Service Recipients in respect of the relevant TS Software and/or IPRs pursuant to or as contemplated by this Paragraph 2 subject to receipt by the Supplier of a confidentiality undertaking in its favour in or substantially in the form set out in Appendix 2 to Annex 12 (*TS Software*) to this Schedule 34 duly executed by the Replacement Supplier;
 - (ii) a licence to use any TS COTS Software and/or TS COTS Background IPRs, on terms no less favourable (including as to indemnification against IPRs Claims) than those on which such software is usually made commercially available by the Supplier; and/or
- (b) use all reasonable endeavours to procure the grant to any Replacement Supplier of a licence to use any Third Party COTS Software and/or Third Party COTS IPRs on terms no less favourable (including as to indemnification against IPRs Claims) than those on which such software is usually made commercially available by the relevant third party.

TS Patents

2.18 Where a patent owned by the Supplier is necessarily infringed by the use of the TS Specially Written Software or TS Project Specific IPRs by the Authority, the Service Recipients or any Replacement Supplier, the Supplier shall hereby grants to the the Authority, the Service Recipients and the Replacement Supplier a non-exclusive, irrevocable, royalty-free, worldwide patent licence to use the infringing methods, materials or software solely for the purpose for which they were delivered under this Schedule 34.

3 LICENCES GRANTED BY THE AUTHORITY

3.1 Not used.

Authority Software, Authority Background IPRs and Authority Data

**ANNEX 32 (TS INTELLECTUAL PROPERTY RIGHTS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

- 3.2 The Authority hereby grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the TS Term to use the Authority Software, the Authority Background IPRs and the Authority Data solely to the extent necessary for performing the Transitional Services in accordance with this Schedule 34, including (but not limited to) the right to grant sub-licences to Sub-contractors provided that:
- (a) any relevant Sub-contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Paragraph 19 (*Confidentiality*); and
 - (b) the Supplier shall not, without the Authority's prior written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Authority.
- 3.3 In the event of the expiry of the TS Term or termination of the Transitional Services, the licences granted pursuant to 3.2 and any sub-licence granted by the Supplier in accordance with Paragraph 3.2 shall terminate automatically on the date of such termination or expiry and the Supplier shall:
- (a) immediately cease all use of the Authority Software, the Authority Background IPRs, and the Authority Data (as the case may be);
 - (b) at the discretion of the Authority (as appropriate), return or destroy documents and other tangible materials that contain any of the Authority Software, the Authority Background IPRs, and/or the Authority Data, provided that if the Authority has not made an election within 6 months of the termination of the licence, the Supplier may destroy the documents and other tangible materials that contain any of the Authority Software, the Authority Background IPRs, and/or the Authority Data (as the case may be); and
 - (c) ensure, so far as reasonably practicable, that any Authority Software, Supplier Background IPRs Authority Background IPRs, and/or Authority Data that are held in electronic, digital or other machine-readable form ceases to be readily accessible from any Supplier computer, word processor, voicemail system or any other Supplier device containing such Authority Software, Authority Background IPRs, and/or Authority Data.

TS Specially Written Software and TS Project Specific IPRs

- 3.4 The Supplier may use and exploit the TS Specially Written Software and/or the TS Project Specific IPRs provided that:
- (a) the Supplier must always offer a price and solution to the Authority which is in accordance with the TS Charges;
 - (b) where the Supplier proposes to exploit the TS Specially Written

**ANNEX 32 (TS INTELLECTUAL PROPERTY RIGHTS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

Software and/or the TS Project Specific IPRs, that it provides a detailed proposal of its plans for exploitation of the TS Specially Written Software and/or the TS Project Specific IPRs and the forecast returns, including (but not limited to) details of the goods and services to be offered by the Supplier which use the TS Specially Written Software and/or the TS Project Specific IPRs, the target markets and territory, the estimated level of orders, the marketing strategy; full details of the estimated costs, prices, revenues and profits; impact assessment on services delivered under Schedule 34; and any other information that would reasonably be required by the Authority to enable them to consider the commercial, legal and financial implications to the Parties of the proposal and any further information which the Authority may reasonably request;

- (c) where the Supplier proposes to discount the prices offered to the Authority in return for the right to exploit the TS Specially Written Software and/or the TS Project Specific IPRs, that it provides clear evidence to demonstrate how the exploitation plans and financial information provided under Paragraph 3.4(b) above have been applied to the price for the Deliverables offered to the Authority and other potential users;

- 3.5 The Supplier acknowledges and agrees that the Authority is under an obligation to comply with procurement Laws and state aid/subsidy control rules when considering proposals for alternative IPR arrangements and the Authority will need to consider its position and approach on a case by case basis.

**ANNEX 32 (TS INTELLECTUAL PROPERTY RIGHTS) to
SCHEDULE 34 (TRANSITIONAL SERVICES)**

Confidential
Contract for the provision of WAN Services

Security Classification (Official)
Contract reference: [REDACTED]

**APPENDIX 1: TS SPECIALLY WRITTEN SOFTWARE AND TS PROJECT
SPECIFIC IPRS**

Name of TS Specially Written Software and TS Project Specific IPRs	Details