



Ministry of Justice

DATED

2024

(1) THE SECRETARY OF STATE FOR JUSTICE

and

(2) BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY

CONTRACT

relating to

provision of LAN Services

Contract reference: con_24092

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.....	11
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 ..	23
10 FINANCIAL AND TAXATION MATTERS.....	23
SECTION D – CONTRACT GOVERNANCE.....	25
11 GOVERNANCE	25
12 RECORDS, REPORTS, AUDITS & OPEN BOOK DATA	25
13 CHANGE	25
SECTION E – SUPPLIER PERSONNEL AND SUPPLY CHAIN.....	27
14 SUPPLIER PERSONNEL	27
15 SUPPLY CHAIN RIGHTS AND PROTECTIONS.....	30
SECTION F – INTELLECTUAL PROPERTY, DATA AND CONFIDENTIALITY	39
16 INTELLECTUAL PROPERTY RIGHTS	39
17 IPRS INDEMNITY	39
18 AUTHORITY DATA AND SECURITY REQUIREMENTS	40
19 CONFIDENTIALITY	41
20 TRANSPARENCY AND FREEDOM OF INFORMATION	43
21 PROTECTION OF PERSONAL DATA	45
22 PUBLICITY AND BRANDING	52
SECTION G – LIABILITY, INDEMNITIES AND INSURANCE	53
23 LIMITATIONS ON LIABILITY.....	53
24 INSURANCE.....	56
SECTION H – REMEDIES AND RELIEF	57

Core Terms

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

25	RECTIFICATION PLAN PROCESS.....	57
26	DELAY PAYMENTS	59
27	REMEDIAL ADVISER.....	59
28	STEP-IN RIGHTS	61
29	AUTHORITY CAUSE.....	63
30	FORCE MAJEURE	66
	SECTION I – TERMINATION AND EXIT MANAGEMENT	68
31	TERMINATION RIGHTS.....	68
32	CONSEQUENCES OF EXPIRY OR TERMINATION	70
	SECTION J – MISCELLANEOUS AND GOVERNING LAW	74
33	COMPLIANCE	74
34	ASSIGNMENT AND NOVATION	77
35	WAIVER AND CUMULATIVE REMEDIES	78
36	RELATIONSHIP OF THE PARTIES	78
37	PREVENTION OF FRAUD AND BRIBERY	79
38	SEVERANCE.....	80
39	FURTHER ASSURANCES	80
40	ENTIRE AGREEMENT	80
41	THIRD PARTY RIGHTS	81
42	NOTICES.....	81
43	DISPUTES.....	82
44	GOVERNING LAW AND JURISDICTION.....	83

Core Terms

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**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. Deed of Guarantee
31. Processing Personal Data
32. Intellectual Property Rights
33. Service Recipients

THIS CONTRACT is made on

2024

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) BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY** a company registered in England and Wales under company number 01800000 whose registered office is at 1 Braham Street, London, E1 8EE (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 local area network (LAN) services.
- (B) On 1 February 2023 the Authority advertised on Find a Tender (reference 2023/S 000-003167), inviting prospective suppliers to submit proposals for the LAN Services which form part of the Authority's ‘Evolve’ portfolio of procurements for ICT services.
- (C) The Supplier is a leading provider of telecommunications and has experience in providing local area network services.
- (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);

- (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 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 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 obligations under this Contract and/or the receipt of the Services by the Authority;

Core Terms

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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.

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;
 - (iii) if the Authority elects to extend the Term beyond the First Extension Period by giving the Supplier at least twenty (20) Working Days' notice before the end of the First Extension Period at the end of the Second Extension Period. For the avoidance of doubt, the First Extension Period and any Second Extension Period should each be for one (1) year.

4.1A If the Authority:

4.1A.1 does not extend the Term for the First Extension Period; or

4.1A.2 extends the Term for the First Extension Period but not for the Second Extension Period; and in either case

4.1A.3 any Sub-contracts relating to Hard LAN Services as set out in Paragraph 3 of Schedule 2 (Service Description) are not novated to the Authority and / or to a Replacement Supplier,

the Supplier will be entitled to Contract Breakage Costs in accordance with Paragraph 3.5 to 3.7 of Schedule 16 (Payments on Termination).

4.1B The duty to mitigate the Contract Breakage Costs as set out in Paragraph 5 of Schedule 16 shall apply.

4.1C For the avoidance of doubt, in the circumstances set out in Clause 4.1A, the Supplier will not be entitled to any Termination Payment other than Contract Breakage Costs.

5 SERVICES

Standard of Services

5.1 The Supplier shall provide:

- (a) the Implementation Services from (and including) the Implementation Services Commencement Date; and
- (b) 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

(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 have been disclosed to the Supplier in the Due Diligence Information (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 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) deliver the Services using efficient business processes and ways of working having regard to the Authority's obligation to ensure value for money.

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
- (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;
- (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);
- (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 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 hereby 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.

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

- (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 Milestone Date for each relevant CPP Milestone; 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.

7.3 Service Credits shall be the Authority's exclusive financial remedy for a KPI Failure except where:

- (a) the Supplier has over the previous 12 month period accrued Service Credits in excess of the Service Credit Cap;
- (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 Service Credit Cap set out in Clause 23.4(b) (*Financial and other limits*)) 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.

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 weighting 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:

- (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.

- 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; and
 - (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.

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

- (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.

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 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.

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 Schedule 5 (*Security Management*); and
 - (iii) comply with all reasonable requirements of the Authority concerning conduct at the Authority Premises, including the security requirements as set out in Schedule 5 (*Security Management*);
- (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
- (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:
 - (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 A and Part D of Schedule 28 (*Staff Transfer*) shall apply;
 - (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 A, 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 Parts A and 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.

Core Terms

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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 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
- (d) the proposed Sub-contractor should be excluded in accordance with Clause 15.22 (*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;
- (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 (*Termination by the Authority of the Soft LAN Services*) 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*);
- (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):

- 15.14.1 where such Sub-Contracts are entered into after the Effective Date, the Supplier will ensure that they all contain provisions that; or

15.14.2 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:

- (a) 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;
- (b) 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 15.14.2(b), the invoice shall be regarded as valid and undisputed for the purpose of Clause 15.14.2(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 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:
 - (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 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.

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.

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 Security Requirements.
- 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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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 (n), 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 (n) 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:
 - (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;
 - (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 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

Core Terms

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 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

Status of the Controller

21.1 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

21.2 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).

21.3 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

21.4 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.

21.5 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 this Clause 21 (*Protection of Personal Data*) and Schedule 31 (*Processing Personal Data*) in relation to paragraphs 1.1 to 1.5, 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*));
 - (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 (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 EU GDPR 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) 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.
- 21.6 Subject to Clause 21.7, 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.
- 21.7 The Processor's obligation to notify under Clause 21.6 shall include the provision of further information to the Controller in phases, as details become available.
- 21.8 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 21.6 (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.
- 21.9 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.
- 21.10 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
- 21.11 The Parties shall designate its own Data Protection Officer if required by the Data Protection Legislation.
- 21.12 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;
 - (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.
- 21.13 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.

21.14 Not used.

21.15 The Parties agree to take account of any guidance issued by the Information Commissioner's Office or any other 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 regulatory authority.

Where the Parties are Joint Controllers of Personal Data

21.16 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

21.17 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*).

21.18 Not used.

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 Notwithstanding the general application of Clauses 21.2 to 21.15 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with Clause 21.17.

Standard Contractual Clauses

21.29 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

Core Terms

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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:

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

Clauses 21.30 to 21.31 below shall apply.

21.30 The Parties agree:

- 21.30.1 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;
- 21.30.2 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;
- 21.30.3 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
- 21.30.4 that if there is any conflict between this Contract and the Standard Contractual Clauses the terms of the Standard Contractual Clauses shall apply.

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

- 21.31.1 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;
- 21.31.2 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;
- 21.31.3 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

21.31.4 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.

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 5.1 (*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 exceed twenty million pounds (£20,000,000);
- (b) the Supplier's aggregate liability in respect of loss of or damage to Authority Data or Losses incurred by the Authority and/or a Service Recipient due to breach of Data Protection Legislation that is caused by Default of the Supplier occurring in each and any Contract Year shall in no event exceed fifteen million pounds (£15,000,000);
- (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

- (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 shall in no event exceed:
- (i) in relation to Defaults occurring in the first Contract Year, an amount equal to 150% of the Estimated Year 1 Charges;
 - (ii) in relation to Defaults occurring during any subsequent Contract Year, an amount equal to 150% 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 150% 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 default, wilful breach of a fundamental term of this Contract or wilful repudiatory breach of this Contract, the references in such Clause to 150% shall be deemed to be references to 200%.

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 (*Termination by the Authority of the Soft LAN Services*) 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

- (iii) in relation to the Compensation Payment, the amount set out in Paragraph 6 of Schedule 16 (*Payments on Termination*) provided that where the Authority terminates the Soft LAN Services (in whole or in part) and any associated Services that are no longer required following termination of the Soft LAN Services pursuant to Clause 31.1A (*Termination by the Authority of the Soft LAN Services*) no Compensation Payment shall be payable by the Authority; 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;
- (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.

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 (and for these purposes a material Default may be a single material Default or a number of Defaults or repeated Defaults (whether of the same or different obligations and regardless of whether such Defaults are remedied) which taken together constitute a material Default),

(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.

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.

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;
 - (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
- (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.

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.

Core Terms

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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.
- 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
 - (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 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 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;
- (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.

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 by the Authority of the Soft LAN Services

31.1A Without prejudice to any other rights or remedies of the Authority howsoever arising, the Authority may partially terminate for convenience the Soft LAN Services (in whole or in part) and any associated Services that are no longer required following termination of the Soft LAN Services by complying with the provisions of Paragraph 11 (Partial Termination of LAN Monitoring Services) of Schedule 25 (Exit Management), provided that the Termination Date shall not occur any earlier than the start of the third Contract Year.

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 exceeds the greater of:

- (i) [REDACTED]
- or

- (ii) the average monthly Charges as calculated by reference to the total Charges in the previous [REDACTED] Service Periods,

and such amount remains outstanding sixty (60) 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*), 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 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 Clause 31.1A (*Termination by the Authority of the Soft LAN Services*) or by the Supplier pursuant to Clause 31.3(a) (*Termination by the Supplier*) or Clause 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) except for any termination pursuant to Clause 31.1A (*Termination by the Authority of the Sof LAN Services*), 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(a) 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.
- 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 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,

Core Terms

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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.

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

- (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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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 or 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;
- (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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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.
- 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 and the Guarantor 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.

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.
- 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.

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 40.3 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 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™ 1st Class or other prepaid, next Working Day	At the time recorded by the delivery service, provided that delivery is between 9.00am and 5.00pm on a	Properly addressed prepaid and delivered as evidenced

service providing proof of delivery.	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).	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		Contract Manager
Address	One Braham Street, London, E1 8EE	Zone 3.19, 3rd Floor, 10 South Colonnade, Canary Wharf E14 4PU
Email		vpn.cmo@justice.gov.uk ,

- 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.

Core Terms

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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.

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)
THE SECRETARY OF STATE FOR)
JUSTICE)

Signature:

Name

(block capitals):

Position:

SIGNED for and on behalf of)
BRITISH TELECOMMUNICATIONS PUBLIC)
LIMITED COMPANY by a director:)

Signature:

Name

(block capitals):

Position:

SCHEDULE 1

DEFINITIONS

Schedule 1 (*Definitions*)

1 DEFINITIONS

- 1.1 In the Contract, unless the context otherwise requires, capitalised expressions shall have the meanings sets 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;
 - 1.3.9 references to "**Paragraphs**" are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided; and

SCHEDULE 1 (Definitions)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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.
- 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):
- (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
 - (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 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.

"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
(*Testing Procedures*),

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;

“Allowable Assumptions”

the assumptions set out in Annex 5 of Schedule 15 (*Charges and Invoicing*);

“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 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);
“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 the closing exchange rate on the Accounting Reference Date;
“Anticipated Contract Life Profit Margin”	has the meaning given in Schedule 15 (Charges and Invoicing)
“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 to it in Paragraph 1.27.1 of Part B of Schedule 13 (Implementation Plan);

"Approval Success"	has the meaning given to it in Paragraph 1.26.1 of this Part B of Schedule 13 (Implementation Plan);
"Approved Sub-Licensee"	any of the following: (a) a Central Government Body; (b) any third party providing services to a Central Government 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;
"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 (Financial Reports and Audit Rights);

“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;

“Audit Rights”

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

“Authoritative Independent Source”

means an entity that has access to verifiable information that can confirm the validity of threat and vulnerability analysis outputs;

“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 will be monitored and maintained under the Services but will not be used by the Supplier 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's Comms Room”

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

the Authority's IT policy in force as at the Effective Date a copy of 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 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 Central Government 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 (*Services Description*)), Schedule 3 (*Performance Levels*), Schedule 4 (*Standards*), Schedule 5 (*Security Management*), Schedule 6 (*Insurance Requirements*), Schedule 13 (*Implementation Plan*), Schedule 24 (*Reports and Records Provisions*), Schedule 25 (*Exit Management*) and Schedule 26 (*Service Continuity Plan and Corporate Resolution Planning*);

“Authority Responsibilities”

the responsibilities of the Authority specified in Schedule 7 (*Authority Responsibilities*);

“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 LAN Services are delivered, including those listed on the Authority Site List;
“Authority Site List”	means the information set out in the ITSM Toolset listing the Authority sites as updated by the Authority and shared with the Supplier via Service Now; ;
“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 including but not limited to the LAN (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”	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 Management System”	means the processes, tools and data used in the ITSM Toolset for the purpose of managing Service 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”	the Authority's baseline security requirements, the current copy of which is contained in Annex 1 (Baseline Security Requirements) of Schedule 5 (<i>Security Management</i>), as

updated from time to time by the Authority and notified to the Supplier;

“Board(s)”

has the meaning given in Schedule 21 (*Governance*);

“Board Confirmation”

means the written confirmation from the Supplier’s Board in accordance with Paragraph 8 of Schedule 18 (*Financial Distress*);

“Breakage Costs Payment”

has the meaning given in Schedule 16 (*Payments on Termination*);

“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”

means the Process of the same name listed in Paragraph 13.1 of Schedule 4 (*Standards*);

“Capacity Management System”

means the processes, tools and data used in the ITSM Toolset for the purpose of managing service capacity. At the Effective Date the technology used in the system is Service Now, but the Authority reserves the right to change the technology at any time during the Term;

“Capacity Plan”

as described in requirement 6.3.2.3 of the Service Management Requirements;

“Catalogue Item”

means a product or service described within the Product and Service Catalogue;

“Catalogue Owner”

means the Authority’s owner of the Product and Service Catalogue as notified to the Supplier by the Authority;

“Central Government Body”

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;
- (b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);
- (c) Non-Ministerial Department; or
- (d) Executive Agency;

“Certificate of Costs”

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

“Change”

any change to this Contract;

“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 (*Change Control Procedure, Service Requests and Projects*);

“Change Control Procedure”

the procedure for changing this Contract set out in Part A of Schedule 22 (*Change Control Procedure, Service Requests and Projects*);

“Change in Law”

any change in Law which impacts on the performance of the Services which comes into force after the Effective Date;

“Change and Evaluation Management Process”

means the Process for managing an Operational Change and listed in Paragraph 13.1 of Schedule 4 (*Standards*);

“Change Management System”

means the processes, tools and data used in the ITSM Toolset for the purpose of managing change. At the Effective Date the technology used in the system is Service Now, but the Authority reserves the right to change the technology at any time during the Term;

“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 (*Charges and*

Invoicing) including any Milestone Payment or Service Charge;

“Class 1 Transaction”

has the meaning set out in the listing rules issued by the UK Listing Authority;

“CNI”

means Critical National Infrastructure;

“Commercially Sensitive Information”

the information listed in Schedule 9 (*Commercially Sensitive Information*) 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) (*Unacceptable KPI Failure*);

“Compensation Payment”

has the meaning given in Schedule 16 (*Payments on Termination*);

“Condition Precedent”

has the meaning given in Clause 4.2 (*Condition Precedent*);

“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 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
(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. Each item has several characteristics including a classification, or type, which indicates what kind of item it is;
“Configuration Management Database” or “CMDB”	means the Authority’s repository for storing the Configuration Items which are a constituent part of the Service Asset and Configuration Management System. At the Effective Date the CMDB is Service Now, but the Authority reserves the right to change the source of the repository at any time during the Term;
“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;
“Continual Service Improvement”	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 for the purpose of managing Continual Service Improvement. At the

Effective Date the technology used in the system is Service Now, but the Authority reserves the right to change the technology at any time during the Term;

“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;

“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;

“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, 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 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*);

“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

	(b) significant impact on the national security, national defence, or the functioning of the UK;
“Critical Performance Failure”	(a) the Supplier accruing in aggregate 2500 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 or Compensation for Unacceptable KPI Failure which meet or exceed the Service Credit Cap; or (c) the performance of the Services falls below the same Service Failure Threshold on three (3) occasions in an six (6) consecutive Service Periods;
“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 National Assembly for Wales), 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); (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 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 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;
“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 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;

“Definitive Media Library” or “DML”	shall be interpreted in accordance with the ITIL as detailed at Paragraph 1.3.13 of this Schedule ;
“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 of sixty (60) days commencing on the relevant Milestone Date;
“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>);
“Deliverable”	an item or feature 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 Process of the same name listed in Paragraph 13.1 of Schedule 4 (<i>Standards</i>);
“Demand Management System”	means the processes, tools and data used in the ITSM Toolset for Demand Management. At the Effective Date the technology used in the system is Service Now, but the Authority reserves the right to change the technology at any time during the Term;
“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 (*Implementation Plan*);

“Device Management and Monitoring Platform”

means the platform comprising the toolset which supports delivery of the Soft LAN Services;

“Device”

means an Authority Asset which is a network device (e.g. network switches, network access control appliances and Wireless Access Points) including any software (including firmware) and components installed on such device (e.g. blades and interface cards);

“Device Software”

any Software installed on a Device;

“DHCP”

means dynamic host control protocol;

“Disclosing Party”

has the meaning given in Clause 19.1 (Confidentiality);

“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 Central Government Body with which the Authority or the Supplier interacts in connection with this Contract;

“Discovery Services”

as described in requirement 6.8.2.1 of the Service Management Requirements;

“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>);
“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 described in Paragraph 1 of Part B of Schedule 13 (<i>Implementation Plan</i>);
“Documentary Deliverable”	deliverables that take 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;

“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 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;

“EAP-TLS”

means extensible authentication protocol - transport layer security;

“Effective Date”

the later of:

- (a) the date on which this Contract is signed by both Parties; and
- (b) the date on which the Condition Precedent has been satisfied or waived in accordance with Clause 4.2 (Condition Precedent);

“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, 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;
“End to End Services”	the Services, together with all other ICT services supplied to the Authority by the Supplier, Other Suppliers, and the Authority’s in-house services;
“End User”	any person authorised by the Authority and/or Service Recipients to use the IT Environment and/or the Services;
“End User Devices”	the hardware utilised by an End User to receive the Services, including, but not limited to desktops, laptops and tablets;
“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;
“EEA”	European Economic Area

“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 be interpreted in accordance with the ITIL as detailed at Paragraph 1.3.13 of this Schedule ;
“Event Management System”	means the processes, tools and data used in the ITSM Toolset for the purpose of managing Events. At the Effective Date the technology used in the system is Service Now, but the Authority reserves the right to change the technology at any time during the Term;
“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

(Service Continuity Plan and Corporate Resolution Planning);

“Extension Period”	a period of a maximum of two (2) years from the end of the Initial Term;
“Field Services”	means the Services described in Paragraph 3.2 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> ;
“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 set out 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;
“First Operational Service Commencement Date”	the Operational Service Commencement Date for the Hard LAN Services and any associated Services comprised in the relevant ATP Milestone;
“Fixed LAN”	as means the infrastructure of the LAN (including all relevant Devices) which provides wired network connectivity, as identified in the CMDB in accordance with Paragraph 2.6 of Schedule 2 (Services Description);
“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 Central Government 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 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 (<i>Staff Transfer</i>);

“Gateway Services”	means a service that is responsible for allowing data to flow from one discrete network to another;
“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;
“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);
“Government Security Classifications”	has the meaning given to it at Government Security Classifications - https://www.gov.uk/government/publications/government-security-classifications ;
“GovWiFi”	means a Wi-Fi authentication service allowing staff and visitors to use a single username and password to connect to guest Wi-Fi services across the public sector;
“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 Guarantee;
“Halifax Abuse Principle”	the principle explained in the CJEU Case C-255/02 Halifax and others;
“Hard LAN Services”	the services as described in Paragraph 3 of Annex A (LAN Technical Requirements) to Schedule 2 (<i>Services Description</i>) and the associated services required to deliver them;
“Health and Safety Policy”	the health and safety policy of the Authority and/or other relevant Central Government Body as provided to the Supplier on or before the Effective Date and as subsequently provided 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”	has the meaning given in requirement 2.1.1.12 of the Technical Requirements;
“Historic”	means in relation to the DMMP, information held in the DMMP at any point from the achievement of Milestone 8 (Soft LAN Services Acceptance Sign Off) to the point immediately before it would become live information;
“Hosting Supplier”	means the supplier(s) responsible for delivering the data centre hosting services;;
“HMRC”	HM Revenue & Customs;
“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”	the Outline Implementation Plan or (if and when approved by the Authority pursuant to Paragraph 3 of Schedule 13 (<i>Implementation</i>

Plan)) the Detailed Implementation Plan as updated in accordance with Paragraph 4 of Schedule 13 (*Implementation Plan*) from time to time;

“Implementation Services”

the implementation services described as such in the Services Description;

“Implementation Services Commencement Date”

the date on which the Supplier is to commence provision of the first of the Implementation Services;

“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. At the Effective Date the technology used in the system is Service Now, but the Authority reserves the right to change the technology at any time during the Term;

“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, 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 three (3) years from and including the Effective Date;

“Initial Upload Date”

means the occurrence of an event detailed in Annex 3 (*Records To Upload To Virtual Library*) of Schedule 24 (*Reports and Records Provisions*) 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 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;
 - (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;

“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 1,875 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 75% of the Service Credit Cap; and/or
- (e) the Supplier not Achieving a Key Milestone within seventy-five (75) days of its relevant Milestone Date;

“IPAM”

means internet protocol address management;

“IP Completion Day”

has the meaning given to it in the European Union (Withdrawal Agreement) Act 2020;

“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, the fourth version of the internet protocol;

“IPv6”

means internet protocol version 6, the most recent version of the internet protocol;

“IT”

information and communications technology;

“IT Environment”

the Authority System and the Supplier System;

“IT Health Check”

has the meaning given in Schedule 5 (*Security Management*);

“IT Service Continuity Management” or “ITSCM”

means the Process of the same name listed in Paragraph 13.1 of Schedule 4 (*Standards*);

“IT Service Continuity Manager”	means the Authority staff member nominated for managing IT service continuity across the Authority's estate;
“IT Service Continuity Plan” or “ITSC Plan”	as described in Paragraph 4 of Schedule 26 (<i>Service Continuity Plan and Corporate Resolution Planning</i>);
“IT Service Continuity Management Plan” or “ITSCM Plan”	has the meaning given in Schedule 26 (<i>Service Continuity Plan and Corporate Resolution Planning</i>);
“ITSCM Event”	means an event that could result in the invocation of the IT Service Continuity Management Plan;
“ITSM Toolset”	means the IT service management system operated and provided by the Authority for management of its services, including the Services and services provided by Other Suppliers;
“Joint Controllers”	where two or more Controllers jointly determine the purposes and means of processing;
“Joint Strategic Partnership Board”	the body described in Schedule 21 (<i>Governance</i>);
“Key Milestone”	the Milestones identified in the Implementation Plan as key milestones and in respect of which Delay Payments may be payable in accordance with Paragraph 1 of Part C of Schedule 15 (<i>Charges and Invoicing</i>) if the Supplier fails to Achieve the Milestone Date in respect of such Milestone;
“Key Performance Indicator”	the key performance indicators set out in Tables 1 and 2 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 (Key Personnel);

“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 (Key Personnel);
“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);
“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 Articles” or “Knowledge Articles”	means the core set of knowledge resources Authority staff and End Users use;
“Knowledge Management Artefact”	the knowledge management artefacts as described in Annex 3 (Records to Upload To Virtual Library) of Schedule 24 (Reports and Records Provisions) and any knowledge management artefacts which the Authority has notified to the Supplier is a Knowledge Management Artefact together with a requirement for each stating the frequency at which the Knowledge Management Artefact is required to be updated and the location in which the Knowledge Management Artefact is to be stored;
“Knowledge Management System”	means those processes, tools and data used by the Authority for the purpose of recording and maintaining knowledge of all services

used by the Authority. . At the Effective Date the technologies used in the system are Service Now, Confluence and SharePoint, but the Authority reserves the right to change the technologies at any time during the Term;

“KPI Failure”

a failure to meet the Target Performance Level in respect of a Key Performance Indicator;

“KPI Service Threshold”

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 (*Performance Levels*);

“LAN”

means the local area networks at the Authority Sites, comprising the Devices in scope of the LAN Services in accordance with Paragraph 2 of Schedule 2 (Services Description) and the associated cabling and Software. “LAN” may be used to mean the local area network at a specific Authority Site, or at more than one Authority Site, or at all Authority Sites, as the context requires;;

“LAN Services”

means the Soft LAN Services and the Hard LAN Services together (in each case) with associated services to be provided by the Supplier to meet the Authority’s requirements (including the service management requirements outlined in Annex B (LAN Service Management Requirements) of Schedule 2 (*Service Description*), the social value requirements outlined in Annex D (LAN Social Value Requirements) of Schedule 2 (*Service Description*) and the security requirements outlined in Schedule 5 (*Security Management*);

“LAN Software”

means the software (including firmware) installed on Devices, and the application(s) which form the DMMP;

“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 Supplier Software, Third Party Software and/or any Specially Written Software;

“License 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. At the Effective Date the technology used in the system is Service Now, but the Authority reserves the right to change the technology at any time during the Term;

“Local ICT Room”

means a room at the Authority Sites that houses system Devices and equipment necessary to deliver End to End Services to End Users at the Authority Sites;

“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”

has the meaning given in requirement 2.1.1.12 of the Technical Requirements;

“Maintenance Schedule”

shall have the meaning set out in Clause 9.4 (Maintenance);

“Major Incident Report”	means the report that is produced in relation to a Major Incident and that describes the nature of the incident and recovery actions taken;
“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;
“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;
“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, 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 1 and 2 of

Part A of Annex 1 of Schedule 3
(*Performance Levels*);

“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/ ;
“Modern Slavery Assessment Tool”	means the modern slavery risk identification and management tool which can be found online at: https://supplierregistration.cabinetoffice.gov.uk/msat
“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>);
“Multi-VLAN”	means a feature supported by network devices which allows the creation and existence of more than one virtual local area network (VLAN);
“NAC”	means network access control;
“NCSC”	the National Cyber Security Centre or any replacement or successor body carrying out the same function;
“NetFlow”	means the network protocol developed by Cisco for collecting IP traffic information and monitoring network flow;
“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;
“Non-Live Environment”	means any ICT Environment used by Supplier or Other Suppliers or the Authority for the development and testing of the End to End Services or Services;
“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-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);
“Object Code”	software and/or data in machine-readable, compiled object code form;
“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 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;

“Open Book Data”

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

“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;

“Open Standards”

means open standards give users permission to copy, distribute and use technology freely or at low cost
<https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles>;

“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 Service Commencement Date”	in relation to each Operational Service, the later of: (a) the date identified in the Operational Services Implementation Plan upon which the Operational Service is to commence; and (b) where the Implementation Plan states that the Supplier must have Achieved the relevant ATP Milestone before it can commence the provision of that Operational Service, the date upon which the Supplier Achieves the relevant ATP Milestone;
“Operational Services”	the services described in the Services Description excluding those described in Annex C (LAN Transition Requirements) to Schedule 2 (<i>Services Description</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”	any supplier to the Authority (other than the Supplier) which is notified to the Supplier from time to time;
“Outline Implementation Plan”	the outline plan set out at Annex 1 of Schedule 13 (<i>Implementation Plan</i>);
“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>);

“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>);
“Performance Failure”	a KPI Failure or a PI Failure;
“Performance Indicators”	the Key Performance Indicators and the Subsidiary Performance Indicators;
“Permitted Maintenance”	has the meaning given in Clause 9.4 (Maintenance);
“Performance Monitoring Report”	has the meaning given in Schedule 3 (<i>Performance Levels</i>);
“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;
“PI Failure”	a failure to meet the Target Performance Level in respect of a Subsidiary Performance Indicator;
“Pilot Testing”	means pilot testing in accordance with the Authority's Service Validation and Testing;
“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”	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 Services Commencement Date and initial period of Early Life Support, which details any risks, issues or defects identified;
“PoE”	means power over ethernet;
“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;
“Problem”	means the cause of one of more Incidents;
“Problem Management”	means the Process of the same name listed in Paragraph 13.1 of Schedule 4 (<i>Standards</i>);
“Problem Management System”	means the processes, tools and data used in the ITSM Toolset for the purpose of managing Problems. At the Effective Date the technology used in the system is Service Now, but the Authority reserves the right to change the technology at any time during the Term;
“Process” or “Processes”	an Authority document (unless the context otherwise requires) that describes processes as they relate to a particular activity identified

in Schedule 4 (Standards) but excluding Standards.

For the avoidance of doubt, this is the definition of "Process" that shall apply to the entire Contract save for Schedule 5 (Security Management), and the definition of "Process" set out in Schedule 5 (Security Management) shall not apply other than to Schedule 5 (Security Management);

"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"

the product and services catalogue developed, maintained and implemented by the Supplier detailing the Services and/or Catalogue Items that can be ordered by the Authority in accordance with the Service Request procedure in Part B of Schedule 22 (*Change Control Procedure, Service Requests and Projects*);

"Product Description"

- (a) a document describing the project Deliverable at the Effective Date in the form set out in Annex 3 of Schedule 13 (*Implementation Plan*);
- (b) a document describing a project Deliverable in the form set out in Annex 2 of Schedule 13 (*Implementation Plan*) and according to content specified by the Authority; or
- (c) a description of a product's purpose, composition, derivation and quality criteria, produced at planning time, once the need for the product is identified, in a form and according to content specified by the Authority;

“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 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 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 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”

appropriate technical and organisational measures designed to ensure compliance with obligations of the Parties arising under Data Protection Legislation and this Agreement, 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*);

“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;

“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;

“QoS”

means quality of service;

“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);

“RADSEC”

means radius secure;

“RBAC”

means role based access control;

“Recipient”

has the meaning given in Clause 19.1 (Confidentiality);

“Records”

means the documents including superseded documents referred to in Annex 2 and Annex 3 of Schedule 24 (Reports and Records Provisions) and as updated from time to time;

“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 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 System”	means the processes, tools and data used in the ITSM Toolset for the purpose of managing releases and deployments. At the Effective Date the technologies used in the system are Service Now, Confluence and SharePoint, but the Authority reserves the right to change the technologies at any time during the Term;
“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) (<i>Standard of Services</i>);
“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);
“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 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;
“Request Fulfilment System”	means the processes, tools and data used in the ITSM Toolset for the purpose of managing request fulfilment. At the Effective Date the technology used in the system is Service Now, but the Authority reserves the right to

change the technology at any time during the Term;

“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);

“RFC”

means ‘request for change’ as defined in ITIL v4 and as may be more particularly described in the Authority’s change management process;

“Risk Mitigation Evidence Artefacts”

means Documentation that is evidence of risk mitigations (e.g. screenshots, log files);

“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 4 of Schedule 15 (*Charges and Invoicing*);

“Risk Treatment Plan”

means a component of the Security Management Plan which deals with the plan for implementing controls that aim to reduce the likelihood or impact of risks;

“Root Cause Analysis”

means an investigation into the underlying or original cause of an Incident or Problem;

“Second Extension Period”

a period of one (1) year from the end of the First Extension Period;

“Second Operational Service Commencement Date”

the Operational Service Commencement Date for the Soft LAN Services and any associated Services comprised in the relevant ATP Milestone;

“Security Audit”

means such regular audits as the Supplier is required to perform for the Authority in order to demonstrate the Services are and remain compliant with the Authority’s security policies, processes, procedures, standards and guidelines, and also National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF);

“Security Case Compliance Statement”	means the Supplier's written statement to the Authority, confirming the Supplier's compliance with any security case issued by the Authority in accordance with the Authority's security management policies, processes, procedures, guidelines, or standards;
“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 1 and 2 of Part A of Annex 1 of Schedule 3 (<i>Performance Levels</i>);
“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”	means a set of tools, data and information that is used to support the Service Asset and Configuration Management. It includes tools for collecting, storing, managing, updating, analysing and presenting data about all service assets and Configuration Items and their relationships. It is a constituent part of the ITSM Toolset. At the Effective Date the technology used in the system is Service Now, but the Authority reserves the right to change the technology at any time during the Term;
“Service Availability”	has the meaning given in Schedule 3 (<i>Performance Levels</i>);
“Service Change”	a change to the LAN and/or the Services in scope of the Authority's Change and Evaluation Management Process, performed by the Supplier;
“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 (*Charges and Invoicing*);

“Service Continuity Plan”

any plan prepared pursuant to Paragraph 2 of Schedule 26 (*Service Continuity Plan and Corporate Resolution Planning*) as may be amended from time to time;

“Service Continuity Services”

the ITSC, disaster recovery and insolvency continuity services set out in Schedule 26 (*Service Continuity Plan and Corporate Resolution Planning*)

“Service Credit Cap”

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

“Service Credits”

credits payable by the Supplier due to the occurrence of one (1) or more KPI Failures, calculated in accordance with Paragraph 3 of Part C of Schedule 15 (*Charges and Invoicing*);

“Service Delivery 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 has overall responsibility for management of the Services;

“Service Design”

defines how the Supplier will design, build and operate the service in life and for the duration of the Contract to ensure the Services operate at the required Performance Indicators, as outlined in Schedule 3 (*Performance Levels*);

“Service Design Package”

has the meaning given in requirement 7.1.1.11 of the Transition Requirements;;

“Service Incident”

has the meaning given in Schedule 3 (*Performance Levels*);

“Service Level Management System”

means the processes, tools and data used in the ITSM Toolset for the purpose of recording and maintaining the Target Performance Levels and attainment against the Performance Indicators. .At the Effective Date the technology used in the system is Service Now, but the Authority reserves the right to

change the technology at any time during the Term;

“Service Management Acceptance Testing”

means service management acceptance testing in accordance with the Authority's Service Validation and Testing;

“Service Management Policies and Processes”

means the service management policies in accordance with ITIL version 3.3 and ISO20000;

“Service Management Requirements”

means the requirements as described in Annex B (LAN Service Management Requirements) to Schedule 2 (*Service Description*);

“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 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; and
- (b) 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 fifth column of tables 1 and 2 in Annex 1 of Schedule 3 (*Performance Levels*);

“Service Portfolio”

shall be interpreted in accordance with the ITIL as detailed at Paragraph 1.3.13 of this Schedule ;

“Service Portfolio Management System”

means the processes, tools and data used in the ITSM Toolset for the purpose of managing the portfolio of services. At the Effective Date

the technologies used in the system are Service Now and Confluence, but the Authority reserves the right to change the technologies at any time during the Term;

“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>);
“Services Description”	the services description set out in Schedule 2 (<i>Services Description</i>);
“Service Transfer Date”	has the meaning given in Schedule 28 (<i>Staff Transfer</i>);
“Service Validation and Testing”	shall be interpreted in accordance with the ITIL as detailed at 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>);
“SIEM”	means security information event management;
“Single Point of Contact” or “SPoC”	means the individual, who is the single point of contact for the relevant activity;
“Sites”	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;

“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 Types”	refers to the Authority Site classification as included in the Authority Site List;
“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’s Requirements;
“Social Value Delivery Plan”	as defined at paragraph 3.1 of Annex D (LAN Social Value Requirements) of Schedule 2 (<i>Services Description</i>);
“Social Value KPI”	The Social Value key performance indicators set out in Table 1 of Part A of Annex 1 of Schedule 3 (<i>Performance Levels</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>);

“Soft LAN Services”	the Services as described in Paragraph 2 of Annex A (LAN Technical Requirements) to Schedule 2 (<i>Services Description</i>) and associated services required to deliver them;
“Software”	Specially Written Software, Supplier Software and Third Party Software;
“Software Supporting Materials”	has the meaning given in Paragraph 2.1(b) of Schedule 32 (<i>Intellectual Property Rights</i>) (Specially Written Software and Project Specific IPRs);
“Solution Design”	has the meaning given in requirement 7.1.2.2 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;
“Specialist Security Services”	means the services provided by the Protective Monitoring supplier, the Digital Forensics supplier(s), and the IT Health CHECK supplier(s);
“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 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;
“SSID”	means service set identifier;

“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/ ;
“Status Report”	as described in Paragraph 7.6 of Schedule 5 (<i>Security Management</i>);
“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 (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 Supplier related to this Contract;
“Subsidiary Performance Indicator”	the performance indicators set out in Tables 3 and 4 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;
“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’s Board”

means the Supplier’s board of directors;

“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
- (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 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 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 (*Charges and Invoicing*);

“Supplier Profit Margin”

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

“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 the software specified as such in Schedule 12 (*Software*);

“Supplier Solution”

the Supplier's solution for the Services set out in Schedule 8 (*Supplier Solution*) 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;
 - (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 (*Financial Distress*);
 - (v) Paragraph 3 of Part B to Schedule 26 (*Service Continuity Plan and Corporate Resolution Planning*);
 - (g) the representation and warranty given by the Supplier pursuant to Clause 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 Clauses:
 - (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); and/orin respect of any security requirements set out in Schedule 2 (*Services Description*), Schedule 5 (*Security Management*) or the Baseline Security Requirements; and/or
- in respect of any requirements set out in Schedule 28 (*Staff Transfer*);
- (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 or the Guarantor;
- (l) the Guarantee ceasing to be valid or enforceable for any reason (without the Guarantee being replaced with a comparable guarantee to the satisfaction of the Authority with the Guarantor or with another guarantor which is acceptable to the Authority);
- (m) a change of Control of the Supplier or a Guarantor 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 the Annex to either Part A or Part B 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 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 6.5(b) / Paragraph 7.7 (b);
 - (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;

- (iii) Supplier COTS Software and Third Party COTS Software is not within mainstream support unless the Authority has agreed in writing.
- (iv) the Supplier fails to patch vulnerabilities in accordance with the Security Requirements; and/or,
- (v) the Supplier fails to comply with the Incident Management Process.

“Supply Chain Map”

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

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

“System Integration Testing”

means systems integration testing in accordance with the Authority's Service Validation and Testing;

“System Testing”

means system testing in accordance with the Authority's Service Validation and Testing;

“TACACS”	means terminal access controller access-control system;
“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 the [Technical Requirements];
“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 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 (*Testing Procedures*);

“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 (*Testing Procedures*) and “**Tested**” shall be construed accordingly;

“Test Schedule”

means a list of activities and their associated timescale for the testing of the ITSC Plans;

“Test Success Criteria”

has the meaning given in Schedule 14 (*Testing Procedures*);

“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 24 (*Reports and Records Provisions*);

“Third Party Beneficiary”

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

“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);

“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);

“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 (*Software*);

“Transferable Assets”

has the meaning given in Schedule 25 (*Exit Management*);

“Transferring Assets”

has the meaning given in Paragraph 7.2(a) of Schedule 25 (*Exit Management*);

“Transferring Authority Employees”

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

“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 Lead”	the Supplier personnel responsible for delivering Transition as described in requirement 7.1.1.4 in Annex C (LAN Transition Requirements) to Schedule 2 (Services Description);
“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;
“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 (LAN Transition Requirements to Schedule 2 (<i>Service Description</i>);
“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>);
“UK”	the United Kingdom;
“UKAS”	means United Kingdom Accreditation Service;
“UK GDPR”	the UK General Data Protection Regulation;
“UK Public Sector Business”	means any goods, service or works provision to UK public sector bodies, including Central Government Departments 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”	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 Annex 3 (Records To Upload To Virtual Library) to Schedule 24 (<i>Reports and Records Provisions</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 Supplier or any third party) releases during the Term;
“User Acceptance Testing”	means user acceptance standards in accordance with the Authority's Service Validation and Testing;
“Valid”	in respect of an Assurance, has the meaning given to it in Paragraph 2.7 of Part B to

Schedule 26 (Service Continuity Plan and Corporate Resolution Planning);

“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 repositories 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>); and
“VRF”	means virtual routing and forwarding;
“Wi-Fi”	means the family of wireless network protocols, based on the IEEE 802.11 standards;
“WAN”	means wide area network;
“WIPS”	means wireless intrusion prevention system;
“Wireless Access Points”	means the Devices that allows other Wi-Fi devices to connect to a wired network;
Wireless LAN (WLAN)	means the infrastructure of the LAN (including the Wireless Access Points and all other relevant Devices) which provides wireless network connectivity, as identified in the CMDB in accordance with Paragraph 2.6 of Schedule 2 (<i>Services Description</i>);
“Wireless Site Survey”	means the process of planning and designing a wireless network, to provide a wireless solution that will deliver the required wireless coverage, data rates, network capacity, roaming capability and QoS;
“WMM”	means wireless multimedia;

SCHEDULE 1 (Definitions)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

“Workaround”

means reducing or eliminating the impact of a Service 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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 2
SERVICES DESCRIPTION

SCHEDULE 2 (Services Description)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Schedule 2 (Services Description)

1 DEFINITIONS

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

2 BACKGROUND AND SCOPE

- 2.1 The LAN is integral to End Users' day-to-day work and therefore is essential to the Authority's and the Service Recipients' ability to deliver services to the public.
- 2.2 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 organisational and technology strategies;
 - Shape and future-proof the Authority's technology infrastructure and services;
 - Ensure technology service contracts are fit for purpose and deliver value for money;
 - Maintain business continuity for End Users; and
 - Create flexibility to suit the changing needs of the Authority and the Service Recipients.
- 2.3 This Schedule 2 sets out the Authority's requirements in relation to each of the following aspects of the Services, as detailed in the Annexes
- (a) Technical Requirements;
 - (b) Service Management Requirements;
 - (c) Transition Requirements; and
 - (d) Social Value requirements.

LAN scope

- 2.4 The Authority Assets in scope of the LAN Services shall be those identified within the CMDB in accordance with Paragraph 2.6 as being within scope of this Contract.
- 2.5 The Authority Assets in scope of the Fixed LAN and the Wireless LAN respectively shall be those identified as such within the CMDB in accordance with Paragraph 2.6.
- 2.6 The details of Authority Assets (including which Authority Assets are in scope of Fixed LAN, WLAN, Soft LAN Services and Hard LAN Services) shall be input into the CMDB by the Supplier in accordance with Paragraph 7.1.2.14 of Annex C (Transition Requirements) and updated by the Supplier in accordance with Paragraphs 6.4.4.3 – 6.4.4.4 of Annex B (Service Management Requirements).

SCHEDULE 2 (Services Description)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Evolving End to End Services

- 2.7 The Authority requires the support of its suppliers of End to End Services to deliver its strategic objectives, including those set out in the Authority's digital strategy and (for network services such as the LAN Services) network strategy.
- 2.8 The Authority's delivery model for the End to End Services is anticipated to evolve during the Term to support its strategic objectives, including (subject to governance) the following anticipated changes in relation to the LAN:
- 2.8.1 **Network operations centre (NOC):** Planned in-source of the Soft LAN Services into scope of the Authority's NOC;
- 2.8.2 **Wi-Fi:** Consolidation of Wi-Fi services and infrastructure (e.g. the HMCTS Wi-Fi service) into the LAN, including integration with the Fixed LAN.
- 2.9 The Supplier shall support the Authority's strategic objectives as set out in Paragraphs 2.7 and 2.8, subject to the Change Control Procedure and (where relevant) Exit Management where any Changes are required to deliver the strategic objectives.

3 SERVICES DESCRIPTION

3.1 Technical Requirements

- 3.1.1 The purpose of the LAN is to securely connect End User devices within the Authority Sites to other devices, and to the Authority's WAN.
- 3.1.2 The Supplier is required to:
- Manage the Authority's LAN infrastructure (including any LAN infrastructure deployed and added to the scope for the LAN Services from time to time);
 - Deploy and maintain structured cabling and patching across the Authority Sites; and
 - Provide Field Services.
- 3.1.3 The Authority seeks to standardise over time on a common architecture for the LAN to simplify future deployment and on-going maintenance. Key objectives are as follows:
- Rationalise vendors in use;
 - Standardise architecture and configuration templates;
 - Integrate Fixed LAN and WLAN infrastructure;
 - Improved access to the LAN for the Authority's LAN service team in terms of visibility of monitoring and status and

SCHEDULE 2 (Services Description)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- Increased performance management of wireless LAN services, including the Wireless LAN, (e.g. by bringing Wi-Fi services into scope of the LAN Services).

3.1.4 The scope of LAN Services includes all Authority Sites with the exception of the datacentre locations.

3.1.5 The technical services are categorised into two service groupings: the Soft LAN Services and the Hard LAN Services.

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

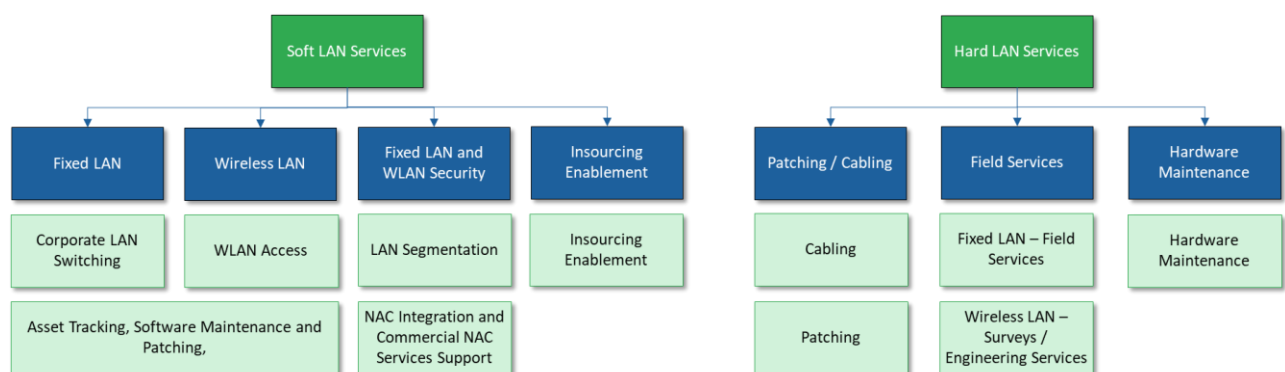


Figure 1: Technical Requirements taxonomy

3.1.7 Soft LAN Services

The Soft LAN Services comprise the remote management (including monitoring, configuration, software upgrades etc.) of the LAN. The Supplier will provision the Device Management and Monitoring Platform (DMMP) to support delivery of the Soft LAN Services. Any in-source of the Soft LAN Services (as described in Paragraph 2.8) may include the transfer of the DMMP from the Supplier System to the Authority; the DMMP will be designed to support such transfer, in accordance with 'insourcing enablement' requirements set out within the Technical Requirements.

3.1.8 Hard LAN Services

The Hard LAN Services comprise the set of services which require attendance at an Authority Site including the supply, installation, physical configuration and decommissioning of Devices and other activities such as conducting surveys, cabling and patching, physical attendance to maintain or repair Devices.

SCHEDULE 2 (Services Description)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

3.1.9 The Authority Assets in scope of the Soft LAN Services and the Hard LAN Services respectively shall be those identified as such within the CMDB in accordance with Paragraph 2.6.

3.1.10 The Technical Requirements are detailed in Annex A (LAN 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 operation's approach to managing technology services; and
- (b) The LAN Service Management Requirements, which are specific to this Contract.

3.2.2 To deliver the Service Management model, 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) Support service management modifications to align with the Authority requirements regarding the management of hardware maintenance and licensing suppliers;
- (d) Operate and manage the tools / systems to provide Service Management in a cost effective and efficient manner;
- (e) Operate and manage tools / systems that provide the Authority with holistic and real-time visibility of the end-to-end services provided; and
- (f) Adopt pro-active monitoring and management of the services, identifying, raising, and working collaboratively with the Authority in the resolution of issues / incidents.

3.2.3 The Service Management Requirements are detailed in Annex B (LAN Service Management Requirements).

3.3 Transition Requirements

3.3.1 The Transition Requirements set out the Implementation Services including the processes and conditions for the effective transition from the Preceding 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:

- **Deliver service value** – the Supplier should seek to deliver the maximum value in terms of the Authority's strategic objectives as early as possible during the Transition process.
- **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 approach is key to this principle.
- **Maintain security** – control risks to security of the Authority Data throughout all aspects of the Implementation Services.
- **Collaborate effectively** – effective collaboration across the Authority's supply chain is essential – including collaboration between the Supplier, the Preceding Suppliers, Other Suppliers and their relevant sub-contractors will be essential during Transition.
- **Deliver on time** – the Supplier shall manage the Transition in accordance with the Milestones, as defined in Schedule 13 (Implementation Plan).
- **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' understanding and documentation of the Authority System and the Preceding Services must be transferred, preserved and used effectively for delivery of the LAN Services.

3.3.3 The Transition Requirements are detailed in Annex C (LAN 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 three key themes:

- Creating employment and training opportunities particularly for those who face barriers to employment and/or who are located in deprived areas, and for people in industries with known skills shortages or in high growth sectors;
- Creating a diverse supply chain to deliver the contract including new businesses and entrepreneurs, start-ups, SMEs, VCSEs and mutuals; and

SCHEDULE 2 (Services Description)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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 (LAN Social Value Requirements).

ANNEXES

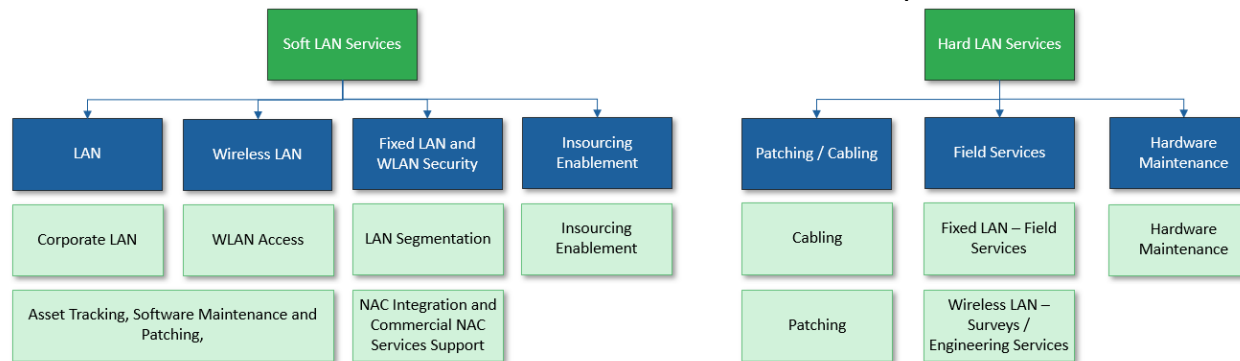
ANNEX A (LAN TECHNICAL REQUIREMENTS)

Schedule 2 (Services Description)

Annex A – LAN Technical Requirements

1. Technical Requirements taxonomy

Figure 2 below is an illustration of the structure of the Technical Requirements, for information only..



taxonomy

Figure 2: Technical requirements

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

2. Soft LAN Services – Technical Requirements

2.1 LAN

2.1.1 Corporate LAN

Design

2.1.1.1	The Supplier shall develop and maintain the architecture and design of the LAN and suggest changes and improvements in line with Good Industry Practice.
2.1.1.2	The Supplier shall integrate the WLAN with the Fixed LAN at all Authority Sites where Fixed LAN and WLAN co-exist.
2.1.1.3	The Supplier shall integrate the LAN with the Authority's WAN in order to establish network connectivity for the LAN.
2.1.1.4	Where there is insufficient capacity to integrate the WLAN and Fixed LAN, the Supplier shall propose a resolution to the Authority of what is required to achieve such integration. (Any implementation of such resolution by the Supplier to be subject to the Change Control Procedure)..
2.1.1.5	The Supplier shall, triggered by new deployments or refresh events, standardise the LAN in terms of Device models (which must be approved by the Authority) to meet the target state architecture described in Paragraph 4.2, such Devices as a minimum support: • user access port speeds of 10/100/1000 Mbps; • power over ethernet to support a range of devices including IP phones, facilities devices such as cameras and access points; • wake-on LAN; • access control integration (administrative access, End User LAN access); and • IPv4 and IPv6.
2.1.1.6	The Supplier shall provide routing capabilities and configuration services aligned to the LAN architecture design approved by the Authority, including: • Point-to-point non-blocking routing; • Route all outgoing LAN traffic to default WAN routers; and • Support as standard for multicast and anycast traffic.
2.1.1.7	The Supplier shall establish a standard set of templates to support consistent Device configuration, aligned to the Standards as detailed in Schedule 4 (Standards) (including MoJ Cyber and Technical Security Guidance) and Good Industry Practice.

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

2.1.1.8	The Supplier shall actively monitor and perform continuous analysis of the configuration and performance of the LAN to establish opportunities to optimise and improve the LAN.
2.1.1.9	The Supplier shall set out a process to standardise the Device configurations across the LAN and manage it on an ongoing basis.
2.1.1.10	The Supplier shall consistently apply design standards and controls across differing vendors and technologies in the delivery of the Services.
2.1.1.11	The Supplier shall, where new or replacement LAN infrastructure is required, agree the make and model of any new Devices with the Authority prior to deploying them to the LAN and ensure the new LAN infrastructure provides support, including but not limited to: • Multi-VLAN trunking; • 802.1x authentication; • Connection of multiple hosts per port; • Multi-domain authentication per port; • VLANs with support including End User voice and video, management; • RADSEC (Radius Secure); • PoE (Power over Ethernet) switches where the minimum standard shall be 802.3af (type1); • Layer 3 routing capabilities, including dynamic routing; • Virtual Routing and Forwarding (VRF) • Application of classification and QoS policies for all network traffic types • Optional support for Switch stacking; and • Role based access control (RBAC) with (terminal access controller access control system) TACACS or radius protocols.
2.1.1.12	The Supplier shall share the detailed specifications and configurations of the Authority Assets of the LAN ("Low Level Designs") with the Authority when making changes to the LAN architecture and/or infrastructure, within five (5) Working Days of making such changes. Any changes to the high-level design describing the overall architecture, major components, their interactions and the description of the LAN ("High Level Design") shall be in accordance with the Change and Evaluation Management Process.

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services*Refresh*

2.1.1.13	The Supplier shall: • Identify the status of all LAN hardware in accordance with Paragraph 2.1.1.14; • Highlight any risks of LAN hardware requiring a refresh; and • Onboard all refreshed LAN hardware.
2.1.1.14	The Supplier shall inform the Authority when Devices' end of sale, end of support and/or end of life dates have been published by the relevant vendors, clearly articulating the key dates and impacts associated with the relevant vendor's end of support lifecycle. These shall be noted by the Supplier in all service reviews with the Authority.

Quality of Service (QoS)

2.1.1.15	The Supplier shall ensure the Devices are capable of prioritising network traffic, as well as the appropriate handling of voice and video data flows as agreed by the Authority.
2.1.1.16	The Supplier shall enable LAN traffic to be identified and marked at the point of entry into the LAN, and subsequent identification and prioritisation to be honoured and maintained to and from the Authority's WAN.
2.1.1.17	The Supplier shall ensure marking and prioritisation approaches for traffic are maintained in accordance with Paragraphs 2.1.1.15 and 2.1.1.16 of this Annex A.

Monitoring and Management

2.1.1.18	The Supplier shall design, provide and maintain the Device Management and Monitoring Platform (DMMP) to: • support the delivery of the Services and to ensure that it is capable of transfer to the Authority.
2.1.1.19	The Supplier shall provide Availability information to the ITSM Toolset through the Device Management and Monitoring Platform.

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

2.1.1.20	The Supplier shall provision the Device Management and Monitoring Platform such that it allows the Soft LAN Services to be securely managed, and allows the Authority to interrogate the Devices.
2.1.1.21	The Supplier shall ensure the Device Management and Monitoring Platform provides monitoring and alerting information to the ITSM Toolset.
2.1.1.22	The Supplier shall implement a centralised management model to allow effective deployment, backup and restore of configuration templates to Devices.
2.1.1.23	The Supplier shall provide the Authority's authorised users of the DMMP with self-service access to the DMMP to be able to query live and Historic metrics, configuration and data points from the LAN as well as reporting functions on-demand.
2.1.1.24	The Supplier shall analyse LAN traffic usage patterns and make recommendations to the Authority, at each Service Period, for achieving optimal usage of the LAN (e.g. for packet discards). Any implementation of such recommendations shall be subject to the Change Control Procedure.
2.1.1.25	Not used
2.1.1.26	The Supplier shall ensure regular configuration backup of all in-scope Devices is carried out and is automated. All backups shall be performed in accordance with the "MoJ Cyber and Technical Security Guidance" Standard.
2.1.1.27	The Supplier shall ensure the Devices store and forward logs both locally, centrally and to the Authority's security logging system.
2.1.1.28	The Supplier shall maintain the logs retention in a manner which is accessible to the Authority. Logs shall be archived and shall be made available to the Authority within twenty-four (24) hours (any day including public holidays) of being requested. The Supplier's shall adhere to the following general principles: • Maintain active raw log data (available on request but as a minimum within 4 hours) • Archive older raw log data and retain for period of a year (available on request but as a minimum within 24 hours) • Maintain SIEM data (i.e. correlated and normalised events) for the previous three full financial years
2.1.1.29	The Supplier shall provide auditable access logs to the Authority.

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

2.1.1.30	The Supplier shall continually conduct checks on the state of the LAN to ensure discovery and management of potential failures. The reports on the checks shall be provided to the Authority in accordance with Schedule 3 (Performance Levels).
2.1.1.31	The Supplier shall operate the Device Management and Monitoring Platform to manage the Devices, including, checking end-to-end connectivity and assisting in troubleshooting of the End to End Services (where attached to the LAN).
2.1.1.32	The Supplier shall centrally apply standards-based policy and configuration across the LAN.
2.1.1.33	The Supplier shall ensure the Services integrate with services and systems of the End to End Services, including network access control (NAC), directory services, domain name system (DNS), dynamic host configuration protocol (DHCP) and IP address management (IPAM), to allow the identification, profiling, fingerprinting, contextualisation of user/device data and policy enforcement.
2.1.1.34	The Supplier shall provide a path for integration of the LAN with broader infrastructure policy orchestration tools.
2.1.1.35	The Supplier shall allow the Authority read only access to the LAN management tooling deployed (including the DMMP).
2.1.1.36	The Supplier shall monitor and log the usage and access to the LAN and the DMMP.
2.1.1.37	The Supplier shall alert the Authority on anomaly events impacting the LAN and/or the DMMP and/or the Services.
2.1.1.38	The Supplier shall enable the Authority to view and export real time data about the LAN on demand, to aid planning, design and troubleshooting activities, including via: • Simple network management protocol (SNMP) access; • NetFlow; • open API, and • standard monitoring and management protocols. Direct Device interrogation shall be controlled in accordance with the relevant Authority policies and procedures to avoid service outages or degradation.
2.1.1.39	The Supplier shall provide the Authority with access to its service management console to allow custom reporting, dashboards, and incident layouts.
2.1.1.40	The Supplier shall enable the Authority to view live and Historic telemetry and metric data about the LAN. Any Historic data should be exportable.
2.1.1.41	The Supplier shall provide regular reports to the Authority, in accordance with Schedule 3 (Performance Levels), including reporting of the degree of LAN utilisation and pro-active advice for further improvement of the LAN.

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

2.1.1.42	The Supplier shall cooperate with Other Suppliers to manage the performance of the End to End Services, and shall undertake such related activities as the Authority may reasonably require to manage such performance, including (where relevant) by: • managing any performance degradation of the End to End Services; • proactively undertaking impact assessments on the End to End Services to identify potential future performance degradation, and providing the results of such assessments to the Authority; and • troubleshooting any performance issues.
2.1.1.43	The Supplier shall provide access to the Authority to relevant tooling and data to perform central monitoring of Devices including, event correlation, auditing and reporting.
2.1.1.44	The Supplier shall support the integration of the LAN with the Authority's dedicated voice network infrastructure, where deployed at Authority Sites.

Operating Changes

2.1.1.45	The Supplier shall provide configuration services subject to a relevant Request and as a Catalogue Item. These must include but not be limited to: • Enabling and disabling of LAN ports; • Configuration of VLANs; • Adaptation of access lists; and • Set-up of configurable features of the LAN Service as agreed with the Authority.
2.1.1.46	The Supplier shall configure LAN switches in line with the LAN architecture approved by the Authority, including: • Allocation of LAN network addressing; • Servers are LAN accessible; • VLANs are setup and enabled; • In-line with security capabilities, ports are enabled; • Layer 2 and layer 3 configurations are implemented; and

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	• Central management and distribution of LAN configurations.
2.1.1.47	Not used
2.1.1.48	The Supplier shall deliver the management of the soft configuration of the Devices.

2.2 Wireless LAN**2.2.1 WLAN Access***Scope*

2.2.1.1	The Supplier shall manage and maintain the WLAN at the Authority Sites and the coverage which the WLAN provides to the End Users located at each Authority Site.
2.2.1.2	The Supplier shall, where required under any relevant Request, provide, deploy, maintain and/or manage additional WLAN components and integrate them with the Fixed LAN.
2.2.1.3	The Supplier shall support the extension of WLAN capability to a range of use cases for End Users where identified and requested by the Authority under any relevant Request.

Design

2.2.1.4	Not used
2.2.1.5	The Supplier shall ensure the WLAN does not prompt the display of a landing page to the End User Devices connecting to it, unless requested by the Authority under any relevant Request.
2.2.1.6	Not used
2.2.1.7	The Supplier shall ensure the Wireless Access Points support integration with network access control and 802.1X and deliver secure, seamless mobility with scalable deployment and performance required for corporate data and voice and video services.
2.2.1.8	The Supplier shall ensure WLAN provides encryption of data in transit, including secure key provisioning.
2.2.1.9	The Supplier shall enable, where supported, at a minimum the detection of rogue wireless access points (including in accordance with Good Industry Practice).

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

2.2.1.10	The Supplier shall ensure that the WLAN is capable of segregating traffic based on End User Device and application, to include a minimum of: • trusted corporate PCs; • un-trusted guest devices; and • authentication and access control.
2.2.1.11	The Supplier shall ensure support for a minimum of four service set identifiers (SSIDs) concurrently.
2.2.1.12	The Supplier shall ensure the WLAN presents the Gov Wi-Fi SSID. If the Supplier requires any information or approvals in order to ensure the Gov Wi-Fi service is provided, the Supplier shall request such details from the Authority.
2.2.1.13	The Supplier shall ensure the WLAN enables seamless wireless roaming between Wireless Access Points with no additional requirement for authentication, for any new deployments at the Authority Sites.
2.2.1.14	The Supplier shall ensure that access to the WLAN does not require the use of browser plug-ins.

New Deployments

2.2.1.15	The Supplier shall, where the Authority requires the deployment/provision of new WLAN infrastructure under any relevant Request, provide the following operational configuration elements: a) virtual LANs; b) broadcast domains; and c) layer 3 switching.
2.2.1.16	The Supplier shall configure any new WLAN deployed under this Contract in line with the requirements from the associated Wireless Site Survey in accordance with Paragraph 3.2.3.6 of Annex B (Service Management Requirements).
2.2.1.17	The Supplier shall ensure any new WLAN deployed under this Contract adheres to the specification approved the Authority during Service Design and documented in the relevant Request.

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

2.2.1.18	The Supplier shall ensure that any new wireless infrastructure provisioned supports the Wi-Fi Alliance certified Wireless Multimedia (WMM) QoS standard. WMM maps the eight 802.1P priority classes on to four access classes within the WLAN. These access classes are background, best effort, video and voice.

Monitoring and Management

2.2.1.19	Not used
2.2.1.20	The Supplier shall provide administrative and logical configuration services for Wireless Access Points and WLAN controllers.
2.2.1.21	Not used
2.2.1.22	The Supplier shall be responsible for: 1. Monitoring the usage and activity of Wireless Access Points; and 2. Reporting on such usage and activity to the Authority each Service Period
2.2.1.23	Not used
2.2.1.24	The Supplier shall report on usage and activity of the WLAN in accordance with [Service Design].
2.2.1.25	The Supplier shall manage the WLAN through the Authority's cloud-based wireless access controllers.
2.2.1.26	The Supplier shall ensure that the Authority has access to the WLAN controllers.

2.3 Asset Tracking, Software Maintenance and Patching**2.3.1 Asset Tracking**

2.3.1.1	The Supplier shall perform asset tracking including analysis, tracking, scanning and reporting on the Authority Assets of the LAN.
2.3.1.2	The Supplier shall co-ordinate asset-tracking activities with the Authority and Other Suppliers, in compliance of relevant Standards detailed in Schedule 4 (Standards).

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

2.3.2 Software Maintenance and Patching

2.3.2.1	The Supplier shall ensure Software, firmware and security patches are applied in accordance with the “MoJ Cyber and Technical Security Guidance” Standard.
2.3.2.2	The Supplier shall support the Authority’s decision making and provide recommendations on Software, firmware and security fix maintenance cycles.
2.3.2.3	The Supplier shall regularly check for availability of vendor updates/upgrades of Device Software and advise the Authority on which updates are needed and perform updates of Device Software as agreed with the Authority.
2.3.2.4	The Supplier shall develop and maintain a Maintenance Schedule which will include the forward schedule of proposed updates to firmware and operating systems in accordance with Clause 9.4 (Maintenance) to ensure that the Authority maintains access to up-to-date vendor features.
2.3.2.5	The Supplier shall undertake Testing aligned with the release management process to ensure proposed vendor updates are stable and suitable for deployment.
2.3.2.6	The Supplier shall support the Authority to validate impacts and any necessary changes on the Authority System including the Authority’s NAC, IPAM and DHCP.
2.3.2.7	The Supplier shall manage and optimise any Software license subscriptions to ensure compliance with vendor terms and conditions in accordance with Clause 5.5 (Supplier Covenants).

2.4 Fixed LAN and Wireless LAN Security

2.4.1 LAN Segmentation

Scope

2.4.1.1	The Supplier shall provide the capability to effectively separate the logical components within a LAN and allow device/user-based policies (security, performance or otherwise) to be applied within those zones to further logically segment subsets of devices.
2.4.1.2	The Supplier shall provide the ability for the Authority to nominate groups of LAN ports at each Authority Site as separate segments to provide traffic separation between routing domains.

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

2.4.1.3	The Supplier shall ensure the “MoJ Cyber and Technical Security Guidance” Standard is strictly followed for the LAN, including zoning within the security model.
2.4.1.4	The Supplier shall provide the Authority with the appropriate level of LAN zoning and segmentation required to meet the security requirements in Schedule 5 (Security Management).
2.4.1.5	The Supplier shall work with the Authority to define the target and transitional segmentation model.
2.4.1.6	The Supplier shall support simplification of the zoning model in conjunction with Other Suppliers.
2.4.1.7	The Supplier shall maintain access and routing in line with the design provided by the Authority and record any exceptions agreed with the Authority.
2.4.1.8	The Supplier shall provide support and maintenance of segregated subnets within the LAN architecture.
2.4.1.9	The Supplier shall be responsible for providing interconnection of the LAN necessary to allow any Device port to access any other Device port and/or the Authority’s Gateway Services where the security policy permits.
2.4.1.10	The Supplier shall consult with the Authority regarding identified or future potential security-related issues affecting the LAN and/or the Services.

2.4.2 NAC Integration and Commercial NAC Services Support*Commercial NAC Services Management*

2.4.2.1	The Supplier shall maintain the commercial NAC solutions used by the Authority (e.g. Cisco ISE and Aruba ClearPass for select prisoner-facing services) for the duration these use cases are still required.
2.4.2.2	The Supplier shall maintain and update access policies to support existing and new access control use cases.
2.4.2.3	The Supplier shall review opportunities to consolidate and converge NAC solutions to simplify ongoing policy management where appropriate and inform the Authority during service reviews.

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services*Authority NAC Integration*

2.4.2.4	The Supplier shall establish and maintain the interface between the LAN as well as the WLAN with the Authority's NAC service to apply required policies to connected devices (public key infrastructure certificate-based access control).
2.4.2.5	The Supplier shall maintain the interface between the WLAN controllers and the Authority's GovWifi NAC services to support Guest Wi-Fi use cases.
2.4.2.6	The Supplier shall ensure that Devices are capable of authenticating to the Authority's NAC, unless otherwise agreed with the Authority.
2.4.2.7	The Supplier shall ensure the Services provide the capability to place End User Devices into different zones and VLANs based on responses from the Authority's NAC service.
2.4.2.8	The Supplier shall ensure that Devices support 802.1X port-based and Wireless NAC and EAP-TLS authentication, unless otherwise agreed by the Authority.

Guest Wireless Access

2.4.2.9	The Supplier shall enable authenticated secure access to the internet for authorised End Users (including guest End Users) using GovWifi at the wireless-enabled Authority Sites.
2.4.2.10	The Supplier shall ensure the LAN securely prevents guest End Users from accessing any of the Authority's systems or data.
2.4.2.11	The Supplier shall ensure the WLAN can support multiple administration portals; e.g: • User self-service; • Local administered, distributing passwords via e-mail/text; and • Temporary lease of guest access.
2.4.2.12	The Supplier shall ensure that the Authority's corporate and guest End Users can be identified separately when using the LAN.

2.5 Insourcing Enablement

The Authority's intention is to insource the Soft LAN Services at an appropriate time during the period of the Contract. The Supplier will need to work with the Authority in designing, planning and executing such activity.

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

2.5.1 Insourcing Enablement

2.5.1.1	The Supplier shall design and build the Device Management and Monitoring Platform to simplify any future transition of Soft LAN Services to the Authority.
2.5.1.2	The Supplier shall ensure that the Device Management and Monitoring Platform is accessible to the Authority.
2.5.1.3	The Supplier shall ensure that the Device Management and Monitoring Platform is logically separate from the Supplier's other customers.
2.5.1.4	The Supplier shall ensure that the Device Management and Monitoring Platform integrates with the Authority's and Other Supplier's service management tools, including: 1. SharePoint; 2. Confluence; 3. ServiceNow; 4. Azure Active Directory; 5. Authority's NAC platform; and 6. Authority's Public Key Infrastructure.
2.5.1.5	The Supplier shall ensure the Device Management and Monitoring Platform provides a graphical user interface which has the capability to display interactive information including multi-vendor Device status.
2.5.1.6	The Supplier shall ensure the Device Management and Monitoring Platform provides an application programming interface (API) for the Authority System to interface with.
2.5.1.7	The Supplier shall ensure that the Device Management and Monitoring Platform can display customisable interactive dashboards including network maps.
2.5.1.8	The Supplier shall ensure that the Device Management and Monitoring Platform provides live (real-time) and Historic data (with a data retention period in accordance with the Cyber and Technical Security Guidance) to the Authority.
2.5.1.9	The Service shall ensure the Device Management and Monitoring Platform provides multi-vendor support for Devices and includes the following capabilities for Devices which support these features: 1. Auditable change logs; 2. Packet capture; 3. Pre-configured alerting and monitoring templates; 4. Pre-configured configuration templates; 5. Carry out routine operational tasks such as backups; 6. Carry out patch management and Software upgrades;

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	7. Automation and zero-touch provisioning; and 8. Alerting functionality for Device status.
2.5.1.10	The Supplier shall provide knowledge and documentation transfer and training to the Authority to enable the Authority to independently operate and manage the Device Management and Monitoring Platform.

3. Hard LAN Services**3.1 Patching / Cabling****3.1.1 Cabling***Scope*

3.1.1.1	The Supplier shall work with the Authority's facilities management function (including Other Suppliers of facilities management) to maintain and manage LAN cabling in line with the Authority's cabling Standards in accordance with paragraph 10 of Schedule 4 (Standards).
3.1.1.2	The Supplier shall work with the Authority's facilities management contractors or the Suppliers' chosen support partners to support the implementation of changes to the LAN in compliance with the Authority's cabling Standards in accordance with paragraph 10 of Schedule 4 (Standards) and the Supplier designs.
3.1.1.3	The Supplier shall maintain cabling standards as specified in paragraph 10 of Schedule 4 (Standards) and advise the Authority of requirements for any new works.
3.1.1.4	The Supplier shall provide cabling services to the Authority where required under any relevant Request, including: • Patching within Local ICT Rooms and/or cabinets located outside any Local ICT Room; • Mapping of structured cabling and remediation of patching/patch records; • Provision of new and/or replacement horizontal and vertical cabling for voice and data services; • Installation of access points; • Provision and/or repair of networks outlets and any cable shielding; and • Provision of structured cabling/patch-panels. The cabling services shall be provided in accordance with the Standards as stated in paragraph 10 of Schedule 4 (Standards).

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

3.1.1.5	The Supplier shall be responsible for provisioning and replacing cabling infrastructure where required at Authority Sites in accordance with the Authority's ICT physical infrastructure Standards stated in paragraph 10 of Schedule 4 (Standards), where required under any relevant Request.
3.1.1.6	The Supplier shall utilise the existing Authority Site infrastructure, including cabling and ducting, where practical, cost effective and subject to the Authority's agreement.
3.1.1.7	The Supplier shall adhere to the Authority's Local ICT Room protocols and cabling colour coding standards in accordance with the Standards as detailed in Schedule 4 (Standards).
3.1.1.8	The Supplier shall, prior to conducting any work in a Local ICT Room, liaise with the relevant Authority facilities management area to ensure the work can be carried out.
3.1.1.9	Working collaboratively with the Authority, relevant Service Recipients or other relevant Government bodies as directed by the Authority, the Supplier shall comply with all building regulations and planning consents applicable when undertaking installation works and cabling services at Authority Sites.
3.1.1.10	The Supplier shall provision, install and maintain the structured cabling (copper and fibre), patch panel(s), Device patching (fly leads), and cabling to Wireless Access Points subject to any relevant Request.
3.1.1.11	The Supplier shall seek the necessary approvals from the Authority and Other Suppliers for the delivery of any work on an Authority Site.
3.1.1.12	The Supplier shall work with the Authority and local facilities management (including any relevant Other Supplier(s) of facilities management) to complete any enablement activities or post-installation remediation activities.

3.1.2 Patching*Scope*

3.1.2.1	The Supplier shall maintain an auditable patch maintenance record. The records shall be available to the Authority upon request.
3.1.2.2	The Supplier shall provide and maintain intra-rack cabling, ad-hoc inter-rack cabling and patching between all Devices within the Authority's Comms Room environments (e.g. switches, servers, interconnects etc.).
3.1.2.3	The Supplier shall provide intra-rack cabling and patching between the Devices, subject to any relevant Request.
3.1.2.4	The Supplier shall manage the relocation of any Devices and racks as required to deliver the Services by coordinating with the Other Suppliers.
3.1.2.5	The Supplier shall provide patch leads under any relevant Request.

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

3.1.2.6	The Supplier shall be responsible for the provision of patch leads to attach any Authority-approved devices to the LAN.
3.1.2.7	The Supplier shall work with the Authority's on-site and remote support to facilitate any patching changes required under any relevant Request.

3.2 Field Services

3.2.1 General

3.2.1.1	The Supplier shall perform onsite support and other necessary activities at the Authority Sites (" Field Services "): a) as required under any relevant Request;; and/or b) as necessary to meet the Performance Indicators and the Standards.
3.2.1.2	The Supplier shall ensure that repeatable Field Services are listed as Catalogue Items, and that such Catalogue Items are reviewed and updated in accordance with Part B (Service Requests and Projects) of Schedule 22 (Change Control Procedure).
3.2.1.3	The Supplier shall supply, manage, commission and decommission Authority Assets within the Local ICT Rooms as required under any relevant Request.
3.2.1.4	The Supplier shall provision, install (including connection of power), maintain and decommission ICT racks as required under any relevant Request. The Supplier shall recycle 100% of the materials where practicably possible on any decommissioned racks.
3.2.1.5	The Supplier shall, prior to conducting any work in a Local ICT Room on the Authority Sites, liaise with the relevant Authority facilities management area to ensure the work can be carried out.
3.2.1.6	The Supplier shall, in order to provide Field Services, follow the Standards for requesting access to Authority Sites and shall adhere to the Standards when attending the Authority Sites.

3.2.2 Fixed LAN – Field Services

General

3.2.2.1	The Supplier shall manage the following components within the Services scope boundary: • Distribution patch panels; and • Interconnect patch panels (to connect to Other Suppliers).

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

3.2.2.2	The Supplier shall be responsible for managing the relocation of Devices and/or racks, subject to prior approval from the Authority and the relevant Hosting Supplier.
3.2.2.3	The Supplier shall manage the interface and specification of enablement work with the Authority's facilities management function (including any relevant Other Supplier(s) of facilities management). Such interface to include power, cooling and racking services.
3.2.2.4	Subject to a relevant Request, the Supplier shall provide: • Cabinet remediation; • Decommissioning and installation of new cabinets; and • Racking of devices within the Local ICT Rooms and/or cabinets located outside the Local ICT Room(s).
3.2.2.5	The Supplier shall provide on-site support where necessary and fulfil Requests for installations, changes and decommissioning in relation to the LAN infrastructure (including Devices).
3.2.2.6	The Supplier shall comply with all building regulations and planning consents applicable when undertaking any installation and cabling works at the Authority Sites.
3.2.2.7	The Supplier shall be responsible for minimising any impact on the Authority's and/or Service Recipients and/or Other Suppliers' infrastructure when delivering the cabling services in any shared areas of the Authority Sites.

Fixed and Wireless LAN Integration

3.2.2.8	The Supplier shall integrate the WLAN components with the Fixed LAN components, including undertaking the physical deployment and configuration activities (under the Authority's direction in accordance with any relevant Request) required for such integration, where Fixed LAN and WLAN co-exist.
3.2.2.9	Where there is insufficient capacity in the LAN to integrate WLAN and Fixed LAN components and where required under Paragraph 3.2.2.8, the Supplier's Impact Assessment shall include the physical deployment and configuration activities required to deploy a resolution to integrate those components.
3.2.2.10	The Supplier shall undertake the physical deployment and configuration activities as directed by the Authority to integrate the LAN with the Authority's WAN in order to establish network connectivity for the LAN.

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services*Refresh*

3.2.2.11	The Supplier shall perform refresh of LAN hardware where the Devices cannot be supported by maintenance agreements (end of service life), where the Devices are at the end of security patching support, or where otherwise requested by the Authority.
3.2.2.12	The Supplier shall: • Develop the forward schedule of LAN refresh; • Ensure incremental deployments for any potential LAN refresh; and • Where undertaking LAN refresh activities, re-examine the deployed architecture and exceptions at the relevant Authority Sites (e.g. cabling, resilience).

Local ICT Room Surveys

3.2.2.13	The Supplier shall be responsible for undertaking surveys of local ICT rooms at Authority Sites, where required under a relevant Request, to include: • Power; • Cooling; • Racking; and • Cabling and to provide the survey report to the Authority.

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**3.2.3 Wireless LAN – Surveys / Engineering Services***General*

3.2.3.1	The Supplier shall provide engineering services under the Product and Service Catalogue (installation, re-location, removal) of the following components: • Distribution patch panels; and • Interconnect patch panels (to connect to Other Suppliers),.
3.2.3.2	The Supplier shall be responsible for undertaking pre- and post-deployment Wireless Site Surveys, where required under a relevant Request, to include: • Floor diagrams showing where Wireless Access Points are advised to be installed; • Installation and cabling works required; • Heat maps; and • Wireless specifications, and to share the survey report with the Authority for approval in accordance with the Document Approval Procedure.
3.2.3.3	The Supplier shall provision and maintain the hardware used to deliver the WLAN.

New Deployments

3.2.3.4	The Supplier shall, as required under any relevant Request, install Authority Assets for the LAN, including; • Wireless Access Points; • LAN switches; and • cabling necessary to connect to the LAN.
3.2.3.5	The Supplier shall ensure that any WLAN components deployed under this Contract integrate with the Fixed LAN.

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

3.2.3.6	The Supplier shall ensure any WLAN deployment provides signal coverage throughout the relevant Authority Site, high speed wireless connectivity and high density, using the best radios and frequencies (e.g. Wi-Fi 6 onwards) possible at all times, all as identified in the relevant Wireless Site Survey.

3.3 Hardware Maintenance**3.3.1 Hardware Maintenance**

3.3.1.1	The Supplier shall maintain the LAN hardware.
3.3.1.2	The Supplier shall maintain each Device in accordance with the maintenance recommendations of the manufacturer / vendor of the Device including firmware and software updates, to ensure that: • There is no degradation in performance of any of the Devices; and • Each Device continues to operate as intended, in accordance with the applicable specification and with the specifications made available by the manufacturer / vendor of the Device.
3.3.1.3	The Supplier shall ensure appropriate maintenance arrangements are in place to underpin the Target Performance Levels for Incident resolution.
3.3.1.4	The Supplier shall develop, maintain and provide to the Authority a Maintenance Schedule for the LAN, with a minimum forward look of twenty-four (24) months.
3.3.1.5	The Supplier shall manage the repair and/or replacement of faulty Devices or directing the LAN maintenance agreement suppliers where appropriate including the management of spare Devices at an appropriate level to meet the Target Performance Levels.
3.3.1.6	The Supplier shall decommission and dispose of the LAN infrastructure subject to a relevant Request or when the equipment is end of life in accordance with the Product and Service Catalogue. The Supplier shall re-use decommissioned Devices where in-life, supportable and reasonable to do so. Any equipment which requires disposal shall be done so in an ethical manner and recycled where appropriate.
3.3.1.7	The Supplier shall align underlying maintenance arrangements to the Performance Indicators, with maintenance extended to all Devices.

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

3.3.1.8	The Supplier shall manage the LAN maintenance supplier contracts for the Devices. For the avoidance of doubt the Supplier shall manage the contracts regardless of the ownership of the Device unless, at the Authority's sole discretion, contract management remains with the Authority.
3.3.1.9	The Supplier shall coordinate the management of Incident and Problem resolution with the LAN maintenance suppliers and manage the relationship with the Authority's WAN supplier to ensure the Performance Indicators are adhered to, including circuit outage at a hosting location.
3.3.1.10	The Supplier shall track Devices and Configuration Items that are covered by hardware maintenance contracts and Devices that are not covered by hardware maintenance contracts.
3.3.1.11	The Supplier shall record the alternative arrangements agreed with the Authority for Devices without formal maintenance contracts; e.g. replace on failure or on-site spares.
3.3.1.12	The Supplier shall propose a strategy (for the Authority's approval) of the appropriate time to purchase hardware maintenance for individual Devices.
3.3.1.13	The Supplier shall source products from vendor approved channels unless otherwise agreed with the Authority.
3.3.1.14	The Supplier shall manage the necessary spare parts for Devices where there is no third-party hardware maintenance contract in place.
3.3.1.15	The Supplier shall operate a spare Device pool sourced from the Authority Site changes / moves.
3.3.1.16	When decommissioning and disposing of LAN infrastructure, the Supplier shall follow the Authority's secure disposal of IT equipment policy.
3.3.1.17	The Supplier shall provide on-site support where necessary and fulfil requests for installations, changes and decommissioning in relation to the LAN and infrastructure (including Devices).
3.3.1.18	The Supplier shall support Authority Asset tracking and management of Devices.

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

4. As-Is and Target Architecture

4.1 As-Is State

At the Effective Date, the Authority Sites will be categorised by the Authority in the Authority Site List as either 'Bronze', 'Silver' or 'Gold' and generally have the Fixed LAN characteristics as outlined in Table 1.

4.1.1 Fixed LAN Characteristics

Characteristic	Bronze	Silver	Gold
Resilience	No resiliency – single point of failure	Resilient core switches	Resilient core switches
Architecture	Access layers (apart from exceptions)	Core and access layers	- Core and access layers - Typically, greater than 20 switch deployments

Table 1: As-Is Fixed LAN characteristics

4.2 Target State Architecture

4.2.1 The Authority seeks to standardise over time on a common architecture for the LAN. Key themes include:

- A flat model at Authority Sites with no hardware resiliency (e.g. small remote offices);
- A collapsed core/distribution model for the remaining Authority Sites, adopting core resilience to reflect importance of associated operations; and
- Where layer 2 extensions are required for campus intra-building connectivity, the Supplier shall manage the LAN and its logical connections and integration to the rest of the network even if the underlying transport is managed elsewhere.

4.2.2 The Authority wishes to standardise on the following architectures through BAU activity, which will likely be triggered by either new site deployments or a major LAN refresh event at a given Authority Site.

ANNEX A (LAN Technical Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**4.2.3 Fixed LAN Characteristics**

Characteristic	Collapsed Core	Split Site Distributed Collapsed Core	Access Only
Architecture	- Hierarchical - Collapsed core and distribution	- Hierarchical - Collapsed core and distribution	Flat
Resiliency	2-layer resiliency, trunked gateway switches	2-layer resiliency, trunked gateway switches	Flat, no resiliency
Technology	- Core and access: Single make and model - PoE	- Core and access: Single make and model - PoE	- Access: Single make and model - PoE
Segregation (Not Exhaustive)	Corporate		

Table 2: Target state Fixed LAN architecture characteristics**4.2.4 WLAN Characteristics**

Characteristic	Collapsed Core	Split Site Distributed Collapsed Core	Access Only
Management	Central controller		
Access	- Guest User e.g. portal authentication - Corporate user e.g. active directory authentication - Other third party - Prison user		
Internet Access	Use office internet common controls		
AP Security	Wireless intrusion prevention system (WIPS)		

Table 3: Target state WLAN architecture characteristics

4.2.5 Architecture Diagrams

The diagrams below illustrate the architecture described in paragraphs 4.2.3 and 4.2.4.

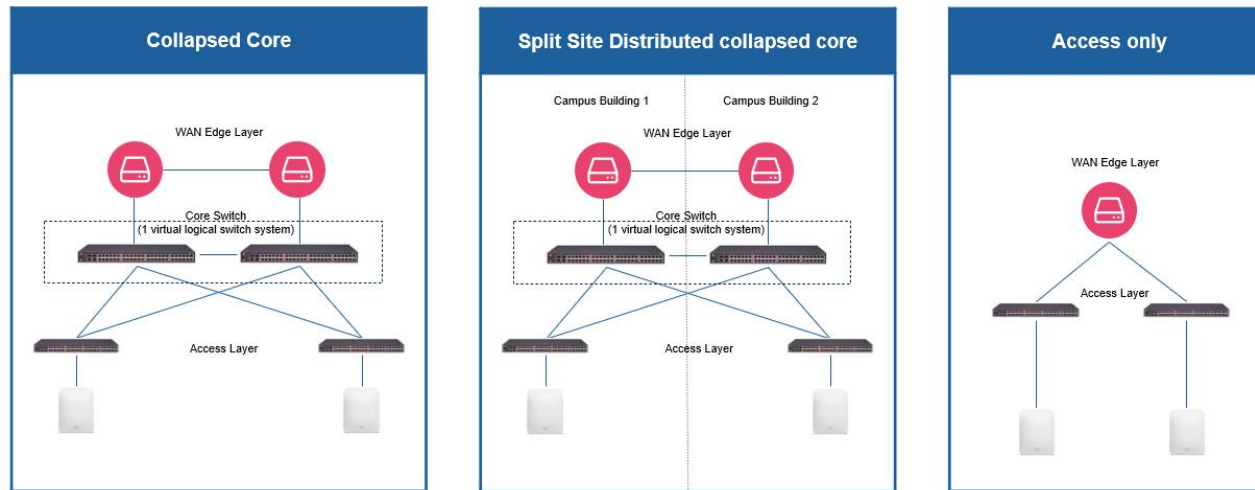


Figure 3: Target state architecture

diagrams

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services



Ministry
of Justice

Schedule 2 (Services Description)

Annex B – LAN Service Management Requirements

These requirements include the baseline Evolve Service Management Requirements (paragraph 6.1 to 6.7) and the requirements specific to the Local Area Network (LAN) Services (paragraph 6.8). Both sets of requirements will apply to the Local Area Network (LAN) Services.

6.1– 6.7 Baseline Evolve Service Management Requirements

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 LAN, Authority System and Authority Data.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

6.1.1.3	General Principles	General	The Supplier shall with regard to Service Management, design, transition, operate and continually improve the Services in accordance with the Authority's processes.
6.1.1.4	General Principles	General	The Supplier shall operate a governance structure that aligns with the Authority's governance structure with appropriate management escalation points.
6.1.1.7.	General Principles	General	The Supplier shall provide support to the Authority, as defined and agreed between the Parties, in order to maintain the Authority's Service Management Policies, and processes.
6.1.1.8.	General Principles	General	The Supplier shall adopt any changes made to the Authority's Service Management Policies, and Processes 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 Authority's demand management processes and shall before engaging with the Authority's business with regard to demand management, procure authorisation in writing to do so from the Authority Representative.
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: 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.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

6.1.8.3.	Service Strategy	Demand Management	The Supplier shall utilise 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 in order to input into detailed business cases for proposed new or changed services, and Projects. Where the Authority decides to proceed the associated changes would proceed through the Change Control Procedure or the Project Work Order process. [DN - this process will be provided at Transition]
6.2.1.2.	Service Strategy	Demand Management	The Supplier shall respond to demand requests from the Authority proposing relevant existing Catalogue Items in the first instance that are contained in the Product and Service Catalogue.
6.2.1.3.			Not Used
6.2.1.4.	Service Strategy	Service Portfolio Management	The Supplier shall ensure the Service Portfolio for the Services is accurate and correct any inaccuracies or missing information identified.
6.2.1.5.	Service Strategy	Service Portfolio Management	The Supplier shall create Service Design Packages for new and changed Services and provide these to the Authority for approval.
6.2.2.1.	Service Strategy	Service Portfolio Management	The Supplier shall, upon commissioning of a new service, document the new Service Design Package and publish these 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 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

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

			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 utilise 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, where possible, End to End Services. The Supplier shall report these emergent risks immediately to the Authority.
6.2.3.4	Service Design	Risk Management	The Supplier shall 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.
6.3.1.1	Service Design	Availability Management	The Supplier shall provide information that reports on the live Availability of the LAN.
6.3.1.2			Not Used.
6.3.1.3	Service Design	Availability Management	The Supplier shall produce a service component failure impact analysis in order to identify the impact of any component failure. This will be produced prior to the LAN going live as part of any transition activities and will form part of the Root Cause Analysis for any Major Incident.
6.3.2.1	Service Design	Availability Management	The Supplier shall provide and operate its own Availability Management system ensuring that it integrates in near real time with the Availability Management System.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

6.3.2.2	Service Design	Capacity Management	The Supplier shall be responsible for monitoring and measuring against pre-agreed thresholds and provide to the Authority both proactive alerting and reactive reporting on the status of the Services in relation to capacity.
6.3.2.3	Service Design	Capacity Management	The Supplier shall produce and submit a quarterly Capacity Plan in accordance with the Authority's Capacity Management process. [DN - this process will be provided at Transition]
6.3.2.4	Service Design	Capacity Management	The Supplier shall provide Capacity information required by the Authority for inclusion into the Capacity Management Information System.
6.3.3.1	Service Design	Capacity Management	The Supplier shall support the Authority in modelling any proposed changes to the Services (including consumption trends) in order to maintain performance against any Performance Indicators.
6.3.3.2	Service Design	Capacity Management	The Supplier shall operate their own Capacity Management System within the DMMP, ensuring that it integrates in near real time with the Authority's Capacity Management System (when available).
6.3.3.3	Service Design	Capacity Management	The Supplier shall manage the availability of IT resources and IT personnel to meet the forecasted demands to support the Service.
6.3.3.4	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. [DN - this process will be provided at Transition]
6.3.3.5	Service Design	IT Service Continuity Management	The Supplier shall ensure that its ITSCM Plan aligns with those of Other Suppliers engaged in the provision of the End to End Services to the Authority.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

6.3.3.6	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.
6.3.4.1	Service Design	IT Service Continuity Management	The Supplier shall define, review and agree with the Authority clear and unambiguous triggers and closure points relating to ITSCM Events.
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 the Supplier's 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 IT Service Continuity Management 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 its SPoC (or a designated substitute if they are unable to attend) attends monthly IT Service Continuity Forums with the IT Service Continuity Manager and records and completes all the Supplier's agreed actions deriving from each Forum.
6.3.4.5			Not used
6.3.4.6	Service Design	IT Service Continuity Management	The Supplier shall ensure that its staff 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 ITSCM plan(s) to ensure that Services are delivered with the agreed recovery objectives.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

6.3.4.8	Service Design	IT Service Continuity Management	The Supplier shall be required to invoke immediately any ITSCM 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 ITSCM 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 manage those risks and capture the output in the ITSCM 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.
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 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 shall state within each ITSCM Plan the Standards to which its ITSCM Plan conforms.
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 agreed closure of an ITSCM Event and where involved in the execution of the ITSCM Plan, the Supplier shall provide the Authority with such information, guidance and assistance as may be reasonably requested to support the production of the Major Incident Report.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

6.3.4.16	Service Design	Service Catalogue Management	The Supplier shall make available and maintain any End User orderable items that supports the Services using the Product and Service Catalogue and maintains performance against any Performance Indicators. End User orderable items are defined by the following: 1. Fixed price/Nil cost; 2. Delivered in a fixed timescale; and 3. Has a predefined fulfilment flow.
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 Authority's ITSM Toolset to provide the Product and Service Catalogue.
6.3.5.1	Service Design	Service Catalogue Management	The Supplier shall follow the Product and Service Catalogue management processes and where the Supplier has provided an alternative Catalogue Item via the Demand Management process, i.e. something not listed in the Product and Service Catalogue, they will procure the Authority's approval and, if given, make it available on the Product and Service Catalogue. [DN - this process will be provided at Transition]
6.3.5.2	Service Design	Service Catalogue Management	The Supplier shall work with the Authority to identify potential 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.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

6.3.5.4	Service Design	Service Level Management	The Supplier shall utilise 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 Schedule 3 (Performance Levels) part B paragraph 1.2, establish a Performance Monitoring Report and Balanced Scorecard Report for the Services.
	Service Design	Supplier Management	The Supplier shall, working with the Authority, ensure that all management and performance information required by the Authority in support of the production of a regular Performance Monitoring Report and Balanced Scorecard Report is made available to the Authority.
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.
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 for a 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 support the development of plans for transition with the Authority for a new service or changes to a service, including:

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

			1. The review of service requirements, service transition plans and any associated documentation; and 2. Resource and delivery time estimates.
6.4.1.1	Service Transition	Transition Planning and Support	Where a transition plan is agreed via the Change Control Procedure, Change and Evaluation Management Process, , or as part of a Project 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	The Supplier shall obtain appropriate approval from the Authority for all Service Design Packages before instigating further service transition activities.
6.4.1.3	Service Transition	Transition Planning and Support	Where agreed via the Change Control Procedure, Change and Evaluation Management Process or as part of 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 a Service the integrity of in situ deliverables, service components and Configurations Items are maintained.
6.4.1.5		Not Used	
6.4.1.6	Service Transition	Transition Planning and Support	The Supplier shall operate their own Transition Planning and Support System ensuring that it integrates in near real time with the Authority's 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 Service Requests, Project Requests, Operational Changes or the Change Control Procedure, and submit these to the Authority.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

6.4.1.8	Service Transition	Change and Evaluation Management	The Supplier shall maintain and provide the Authority with a list of nominated approved Supplier Staff who are authorised to submit an RFC.
6.4.1.9	Service Transition	Change and Evaluation Management	The Supplier shall ensure that all RFCs submitted contain the appropriate level of details 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, including: 1. Emergency CAB; 2. Reviews of RFCs; and 3. Major Incident fix retrospective change approvals.
6.4.2.1	Service Transition	Change and Evaluation Management	The Supplier shall provide all information relating to pre-approved Changes to the Authority for inclusion in the Authority's ITSM Toolset.
6.4.2.2	Service Transition	Change and Evaluation Management	The Supplier shall inform the Authority of any partial or full failure of a pre-approved Change.
6.4.2.3	Service Transition	Change and Evaluation Management	The Supplier shall assess the environmental impact of the introduction of any new service, or any architecturally significant change to any existing Services, as part of the Change and Evaluation Management Process. [DN - this process will be provided at Transition]
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 utilise the Authority's Change Management System.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 service knowledge management system, to include: 1. Methods to resolve Incidents; 2. Known errors; 3. Minimum data set information; 4. Self help articles 5. Frequently asked questions; 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 Authority's Knowledge Management System.
6.4.3.1	Service Transition	Knowledge Management	The Supplier shall utilise the Authority's Knowledge Management System and it's ITSM Toolset.
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.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

6.4.3.4	Service Transition	Release and Deployment Management	The Supplier shall support the Authority in maintaining and updating the release schedule, which is a planned timeline or calendar that outlines the dates for releases.
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 to the Authority and/or Service Recipients is minimised.
6.4.4.2	Service Transition	Release and Deployment Management	The Supplier shall utilise the Authority's Release and Deployment Management System.
6.4.4.3	Service Transition	Service Asset and Configuration Management	The Supplier shall ensure that all Configuration Items, including all active, non-active and retired Authority Assets in scope for the LAN are identified and relationships recorded and reported to the Authority in the Authority's Service Asset and Configuration Management System. For the avoidance of doubt, any non-active Authority Assets that are unknown to the Supplier and are not discoverable remotely are excluded from this requirement.
6.4.4.4	Service Transition	Service Asset and Configuration Management	The Supplier shall maintain accurate and up-to-date records of all Configuration Items, Assets and Authority Assets including spares, both past and present, and their current status.
6.4.4.5	Service Transition	Service Asset and Configuration Management	The Supplier shall utilise the Authority's Definitive Media Library system (when available).
6.4.4.6	Service Transition	Service Asset and Configuration Management	The Supplier shall ensure that the Authority's Service Asset and Configuration Management system is updated in near real time as a result of any process, including Incident Management, Change and Evaluation Management, Request Fulfilment, Release and Deployment Management, License Management and Compliance, and Service Asset and Configuration Management.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

6.4.5.1	Service Transition	Service Asset and Configuration Management	The Supplier shall utilise the Authority's Service Asset and Configuration Management System.
6.4.5.2	Service Transition	Service Asset and Configuration Management	The Supplier shall ensure that only software that is contained in the Definitive Media Library is deployed within the Authority estate
6.4.5.3	Service Transition	Service Asset and Configuration Management	The Supplier shall securely remove and dispose of assets identified as redundant and 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	License Management and Compliance	The Supplier shall be responsible for the provision and renewal of all Software licences and certificates for the service in accordance with Clause 3.2(j) (Warranties).
6.4.5.6	Service Transition	License Management and Compliance	The Supplier shall capture, manage and monitor licence usage and, with reference to the information contained within the Definitive Media Library, ensure that such usage is legal and provides this information each Service Period to the Authority. As a minimum, the information shall include: • Product; • Edition; • Version details of the software licences consumed and utilisation; • Licence entitlement details including term; and • Hardware information relevant to licence consumption, such as processor type and/or power, number of cores, and virtualisation configuration details.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

6.4.5.7	Service Transition	License Management and Compliance	The Supplier shall be responsible for the ongoing management and monitoring of 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	License Management and Compliance	The Supplier shall ensure that software deployed as part of the service is efficiently, effectively and when possible, automatically removed or redeployed across the IT Environment as required.
6.4.6.2	Service Transition	License 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	License Management and Compliance	The Supplier shall operate their own License Management System ensuring that it integrates with the Authority's LicenSe Management System and the ITSM Toolset (when available).
6.4.6.4	Service Transition	License Management and Compliance	The Supplier shall, unless agreed with the Authority, consolidate versions of client software to the latest versions listed within the Definitive Media Library.
6.4.6.5	Service Transition	Service Validation and Testing	For 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	For Service Validation and Testing, the Supplier shall support the Authority in the planning, design, implementation, execution and reporting of: 1. User acceptance Testing;

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

			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.
6.4.7.1			Not Used.
6.4.7.2	Service Transition	Service Validation and Testing	The Supplier shall, when required by the Authority, produce a programme/project test strategy and/or project/release test plan and submit to the Authority for approval.
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 they are responsible for, irrespective of whether the tests were successful or unsuccessful.
6.4.7.5			Not Used.
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 Other Suppliers in the testing of hardware, software and applications as requested by the Authority.
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.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 identified as necessary in the Test Strategy/Test Plan, and shall ensure that the Non-Live Environment is representative of the Live Environment.
6.4.7.13	Service Transition	Service Validation and Testing	The Supplier shall ensure that 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 available the Supplier's Non-Live Environment to Other Suppliers, where requested by the Authority.
6.4.7.15	Service Operation	Event Management	The Supplier shall provide defined event thresholds for the Services to the Authority for approval.
6.4.7.16	Service Operation	Event Management	The Supplier shall be responsible for the investigation and resolution of any events that have exceeded a pre-defined event threshold.
6.4.7.17	Service Operation	Event Management	The Supplier shall ensure that the Authority is informed of any corrective action taken to address an event and that the relevant records are updated.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

6.5.1.1	Service Operation	Event Management	The Supplier shall operate their own Event Management System within the DMMP ensuring that it integrates 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, that have exceeded a pre- defined threshold.
6.5.1.3	Service Operation	Incident Management	The Supplier shall deliver Incident management to the Performance Indicators and Incident Resolution Deadline as defined in Schedule 3 (Performance Levels).
6.5.1.4	Service Operation	Incident Management	The Supplier shall ensure that the Incident management process within their 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 provide an approved Workaround 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.
6.5.2.2	Service Operation	Incident Management	The Supplier shall, following notification of an Incident, schedule and perform resolution activities with the End User in accordance with the Incident Management Process.
6.5.2.4	Service Operation	Incident Management	The Supplier shall update the Incident record with all relevant information within the Authority's ITSM Toolset relating to the incident in accordance with the Incident management process.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

6.5.2.5	Service Operation	Incident Management	The Supplier shall provide progress updates on all current Incidents in accordance with the Authority's Incident management process. [DN - this process will be provided at Transition]
6.5.2.6	Service Operation	Incident Management	The Supplier shall ensure attendance to any technical Incident management bridge calls and management bridge calls (if necessary) with skilled and experienced staff who understand the service being provided.
6.5.2.7	Service Operation	Incident Management	The Supplier shall utilise the Authority's Incident Management System
6.5.2.8	Service Operation	Problem Management	The Supplier shall deliver Problem Management in accordance with the Performance Indicators set out in Schedule 3 (Performance Levels).
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, 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 provision of Root Cause Analysis Reports within 10 working days of Authority request.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

6.5.3.4	Service Operation	Problem Management	The Supplier shall utilise the Authority's Problem Management System
6.5.3.5	Service Operation	Problem Management	The Supplier shall provide the Authority with all appropriate information on Incidents, Problems, known errors and approved Workarounds.
6.5.3.6	Service Operation	Request Fulfilment	The Supplier shall action each Service Request they receive from the Authority in accordance with the associated lead time specified within the Product and Service Catalogue and maintain performance against any Performance Indicators.
6.5.3.7	Service Operation	Request Fulfilment	The Supplier shall notify the Authority of any anticipated failure to fulfil a Service Request in accordance with the associated lead time.
6.5.3.8	Service Operation	Request Fulfilment	The Supplier shall utilise the Authority's Request Fulfilment System.
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, and document these within the associated knowledge article.
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.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 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 suitable service desk capability for the logging, tracking and escalation of Incidents.
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 life cycle.
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

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

			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.
6.5.6.4	Continual Service Improvement	General	The Supplier shall utilise 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 and their required permission level.
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 Services features can be delivered through the Authority's self service portal.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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, submitting the documentation to the Authority for approval.
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 and compliance with the Performance Indicators.
6.6.1.3	Service Operation	Technical Management	Where there are any changes to software, the Supplier shall inform the Authority with reasonable notice in order to impact assess and mitigate any risks.
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.
6.7.1.1	Service Operation	Technical Management	Where support for hardware, firmware or software used for the provision of the service is to be withdrawn during Term and within a 2 year period post end of the Term, the Supplier shall notify the Authority with reasonable time to ensure that a review commences and that replacement deliverable(s) are identified, tested and made available before the manufacturer withdraws support.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

6.7.1.2	Service Operation	Technical Management	The Supplier shall co-ordinate with the Authority and Other Suppliers of the service components required for inclusion in client builds necessary to ensure continuity of the service.
6.7.1.3			Not Used.
6.7.1.4	Service Lifecycle Management	Architecture Management	The Supplier shall provide enterprise architecture services for their environments 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 " Deployed Architecture ") of the Services 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.
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 every 6 months.
6.7.2.2	Service Lifecycle Management	Architecture Management	The Supplier shall perform architecture impact assessments upon the Deployed Architecture for the Services in accordance with the Authority's Change and Evaluation Management Process.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 with Good Industry Practice.
6.7.2.6	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 Good Industry Practice.
6.7.2.7	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 the Standards.
6.7.2.8	General Principles	Collaboration	The Supplier shall 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, to 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, 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

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

			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.
6.7.2.9	General Principles	Collaboration	The Supplier shall work with the Authority and Other Suppliers in the development, implementation and operation of inter-supplier governance processes and meeting structures.
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.
6.7.2.11	General Principles	Personnel	The Supplier shall ensure that all Supplier Personnel meet the security requirements as detailed in Schedule 5 Annex C Section 9

6.8 Service Design**(a) 6.8.1 Supplier Management**

The Authority is seeking a Supplier to manage licence and maintenance suppliers.

It is the intent that the Supplier will have a fully operable supplier management capability that is measurable and adheres to these requirements and the baseline Evolve Service Management Requirements.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**(b) 6.8.2 LAN licence and maintenance supplier management**

6.8.2.1	AN Specific Requirement	LAN licence and maintenance supplier management	The Supplier shall provide Discovery Services that include: • Validation of the LAN licence and maintenance suppliers' inventory of licences and maintenance agreements and collection of relevant information on them; and • Onboard, validate and manage the inventory of licences and maintenance agreements associated with the Service.
6.8.2.2	LAN Specific Requirement	LAN licence and maintenance supplier management	The Supplier shall provide implementation services that include: • Definition, set up and operation of the operational interfaces and processes between the Supplier and the LAN licence and maintenance suppliers in regard to the scope that the Supplier will be managing these suppliers; • Development of an Operational Interlock Document using data collected through Discovery Services that identifies operational and escalation interfaces with the LAN licence and maintenance suppliers; • Management of communications between the Authority, the Supplier and the LAN licence and maintenance suppliers, with the objective that the relevant processes work seamlessly.
6.8.2.3	LAN Specific Requirement	LAN licence and maintenance supplier management	The Supplier shall maintain the Authority's Service Asset and Configuration Management System and ITSM Toolset with detail of the licences and maintenance agreements provided by Other Suppliers for the Services, when there are changes, additions or terminations of the relevant services.
6.8.2.4	LAN Specific Requirement	LAN licence and maintenance supplier management	The Supplier shall inform the Authority in a timely manner when maintenance agreements / licences require renewal.

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

6.8.2.5	LAN Specific Requirement	LAN licence and maintenance supplier management	The Supplier shall provide Service, Order, Change and Service Request Management Services that include: • Management of changes requested by the Authority regarding the services provided by the LAN licence and maintenance suppliers, including new service orders, changes to existing services and disconnects; • Notifying the Authority of the status and completion of Service Requests to the LAN licence and maintenance supplier management suppliers; • Provision directly or obtain from the relevant licencing and maintenance arrangements to support the operational take on for new Service Requests and Changes.
6.8.2.6	LAN Specific Requirement	LAN licence and maintenance supplier management	The Supplier shall provide Incident Management and Problem Management services that include: • Raising tickets for identified service Incidents related to LAN licence and maintenance suppliers; • Managing any Severity 1 Service Incidents or are considered by the Authority as Major Incidents; • Coordinating ticket updates to the Authority's Service Desk for proactively or reactively identified service Incidents related to the LAN licence and maintenance suppliers with the relevant third parties; • Managing the testing and validation of any Incident resolution across the Supplier and the LAN licence and maintenance suppliers, to ensure that the Incident is resolved successfully and within any agreed performance levels; • Managing escalations to secure a satisfactory outcome where the escalation is in relation to the LAN Infrastructure Suppliers; • Identification and obtaining reporting of recurring issues related to the LAN licence and maintenance suppliers' performance and operational process framework; and

ANNEX B (LAN Service Management Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

			• Performing Root Cause Analysis and known error management for all service Incidents and areas of concern that are in scope of the LAN licence and maintenance suppliers.
6.8.2.7	LAN Specific Requirement	LAN licence and maintenance supplier management	The Supplier shall provide monitoring services that include: • Pro-actively identifying when licenses/maintenance provided by the LAN licence and maintenance suppliers are not working correctly; and • Trend analysis on license volume and types provided by the LAN licence and maintenance suppliers.



**Ministry
of Justice**

Schedule 2 (Services Description)

Annex C – LAN Transition Requirements

7. Service Transition

7.1 Transition Planning and Mobilisation

7.1.1.1	The Supplier shall manage the Transition in accordance with the timescales set out in the Detailed Implementation Plan provided in Annex 1 Outline Implementation Plan of Schedule 13 (Implementation Plan) and Schedule 14 (Testing Procedures) and will ensure that the Preceding Services are fully replaced to Achieve the Key Milestone M10 - Fixed LAN and Wireless Services Transition.
7.1.1.2	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 the successful Transition of services.

ANNEX C (LAN Transition Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

7.1.1.3	In order to Achieve the Key Milestone M2 Contract Setup Complete' the Supplier shall have appointed a Transition Lead and appropriately sized team with experience, and a record of delivery in transitions of comparable size and complexity to the Transition being undertaken
7.1.1.4	In order to Achieve the Milestone 'M2 Contract Setup Complete' the Supplier shall have agreed the Detailed Implementation Plan with the Authority, such agreement in accordance with the provisions and deliverables of Schedule 13 (Implementation Plan) and Schedule 14 (Testing Procedures)..
7.1.1.5	In order to Achieve the Milestone 'M2 Contract Setup Complete' the Supplier shall have appointed an experienced HR Lead who shall be responsible and accountable for managing the people transition activity including onboarding activities and resultant changes to any existing schemes as a result of transfer under employment regulations (where applicable), training requirements and/or support for employees joining.
7.1.1.6	The Supplier shall comply with Good Industry Practice with respect to recruitment and shall keep the Authority updated on resourcing needs and fulfilment throughout the Transition, including mobilisation.
7.1.1.7	The Supplier shall operate an effective risk management approach which aligns with the Authority's risk management processes and procedures, it will: a) seek to resolve all risks to Transition, issues, and Defects that it identifies; and b) shall notify the Authority within two Working Days of a risk or issue being identified where: (i) a risk or issue may cause a delay to Transition or ongoing service requests or projects; (ii) a risk or issue could result in stranded services (stranded services being those services provided through agreements due to come to an end before a suitable replacement service is provided); (iii) the Supplier is unable to resolve the relevant risk or issue that could impact the service; (iv) a risk or issue may cause a delay to Transition or ongoing service requests or projects, the Supplier will present the Authority with a remediation plan within five Working Days, outlining options and a recommendation, as to how the impact of the risk or issue can be mitigated. This requirement does not affect the Supplier's obligations with regard to Notifiable Defaults and Rectification Plans.
7.1.1.8	In order to Achieve Key Milestone M5 'Hard LAN Services Support Service Acceptance' and Key Milestone 'M8 Soft LAN Services Acceptance Sign Off'. The Supplier shall develop an approach to knowledge transfer which will support the delivery of the Detailed Implementation Plan and its associated Transition outcomes.

ANNEX C (LAN Transition Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

7.1.1.9	In order to Achieve Key Milestone M5 'Hard LAN Services Support Service Management Acceptance' and Key Milestone 'M8 Soft LAN Services Support Service Management Sign Off. the Supplier shall produce training material and knowledge articles in accordance with Schedule 24 (Reports and Records Provision) and deliver training for a period which will be agreed with the Authority. The training will be delivered to the Authority's service management teams, to ensure the Authority's service management staff are provided with the knowledge required to deliver their role in service management. The Supplier shall provide the draft training material to the Authority's Service Owner for approval (not to be unreasonably withheld or delayed) and shall make any amendments reasonably requested by the Authority. The training materials and knowledge articles will be provided to the Authority for approval in accordance with Part B of Schedule 13 (Implementation Plan).
7.1.1.10	In order to Achieve Milestone 'M2 Contract Setup the Supplier will provide the Authority with an in-flight project and interim service request report within twenty Working Days of the Effective Date, the format of the report will be agreed with the Authority within this period. 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 by the Supplier under this Contract through to completion.
7.1.1.11	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; (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".
7.1.1.12	The Supplier shall, in accordance with the Detailed Implementation Plan, agree a baseline list of Fixed LAN and Wireless LAN Authority Assets and configuration items.

ANNEX C (LAN Transition Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

7.1.2 Design and Delivery

7.1.2.1	The Supplier shall seek approval from the Authority's Technical Design Authority for all High-level Designs (and any updates to them) before it proceeds with any subsequent delivery activities outlined in the Detailed Implementation Plan.
7.1.2.2	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 Preceding Service and d) how it interfaces with high and low-level technical documentation. When Approved, this Documentary Deliverable shall be the "Solution Design".
7.1.2.3	In accordance with the timescales in the Implementation Plan, the Supplier shall provide the Authority with a forward schedule of change outlining a schedule of when the LAN Services will commence as Operational Services. The Supplier shall provide the Authority with a forward schedule of change at the date agreed within the Detailed Implementation Plan, outlining a schedule of when the Services will commence.
7.1.2.4	In order to Achieve an Operational Service Commencement Date, the Supplier is required to Achieve the relevant ATP Milestone in respect of the particular services and Deliverables for which the relevant Operational Service Commencement Date is sought through the successful completion of the cutover to service commencement gate which forms part of the Authority's Transition Framework
7.1.2.5	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;

ANNEX C (LAN Transition Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	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 7.2.1.10; 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 7.2.1.6. 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”).
7.1.2.6	For the purposes of requirement 7.2.1.5, 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.
7.1.2.7	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.
7.1.2.8	The Supplier shall participate and contribute to post implementation reviews as requested by the Authority, including when each Operational Service Commencement Date is achieved
7.1.2.9	In order to support the Detailed Implementation, Plan the Supplier shall provide the Authority with the below release documentation and activities: a) Release plans;

ANNEX C (LAN Transition Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	b) Release packages; and c) Implementation and assurance activities associated with the scheduled release.
7.1.2.10	The Supplier shall plan and implement release activity to ensure that any business disruption is minimised, and the Authority's release management processes are followed.
7.1.2.11	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).
7.1.2.12	The Supplier shall, in accordance with the Detailed Implementation Plan, provide the Authority with a communication plan which addresses the communication approach for each stakeholder and stakeholder group. The Supplier shall engage with the Buyer 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
7.1.2.13	The Supplier shall provide Documentation to describe the Deployed Architecture of the Services and make them available to the Authority within three (3) months of the Effective Date.
7.1.2.14	The Supplier shall provide Authority approved IT Service Continuity Management (ITSCM) awareness and training for all their ITSCM related personnel within three (3) months of the Effective Date.
7.1.2.15	The Supplier shall, within the timescales required under the Implementation Plan, complete an upload of the baseline list of Authority Assets and configuration items which form the LAN into the CMDB, including conducting due diligence on such baseline list and subject to Approval of the final list following such due diligence.
7.1.2.16	The Supplier shall, within the timescales required under the Implementation Plan, provide the Authority with a Documentary Deliverable which: a) summarises the completion of the Transition and the associated milestones;

ANNEX C (LAN Transition Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	b) list all the activities completed and the associated deliverables; c) documents any issues that were encountered during Transition and how they were resolved; d) details the knowledge transfer activities that took place e.g. training sessions or documentation handovers; e) documents the acceptance sign-off from the Authority, confirming that The Transition is complete; f) details metrics that demonstrate the success of the transition process; g) highlight key lessons learned during Transition and recommendations for future transition projects; h) outline any remaining actions or follow-up tasks. When Approved, this Documentary Deliverable shall be the “Transition Closure Report”.

7.1.3 Transition General

7.1.3.1	The Supplier shall, on a weekly basis report 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 for Transition, and the dates for completion of the Deliverables and such other information as the Authority may request.



Ministry
of Justice

Schedule 2 (Services Description)

Annex D: Social Value Requirements

Prj_9723

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 4 – 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 for people in industries with known skills shortages or in high growth sectors.
	Increase supply chain resilience and capacity	MAC 3.1: Create a diverse supply chain to deliver the contract including new businesses and entrepreneurs, start-ups, SMEs, VCSEs and mutuals.
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.
- 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 5 below.

Table 5 – 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.
Increase supply chain resilience and capacity	For each of the following categories: i. start-ups ii. SMEs iii. VCSEs iv. mutuals;

	The number of Sub-Contract opportunities awarded under the Contract. The value of Sub-Contract opportunities awarded under the Contract in pounds sterling. Total spend under the Contract, as a percentage of the Charges Number of people-hours of learning interventions delivered under the Contract, by UK region.
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 6 – 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 KPI for social value delivery specified in Schedule 3 (Performance Levels) of this Contract will be calculated based on evaluation of targets in accordance with paragraph 4.4, using the following template:

Table 7 – Template for evaluation of specific reporting metrics

Reporting metric	Delivery period	Performance thresholds				Actual Delivery	% Delivery	Rating
		Good	Approaching target	Requires improvement	Inadequate			

ANNEX D (LAN Social Value Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

[Insert]	Q [insert] [Year]	[Threshold]	[Threshold]	[Threshold]	[Threshold]	[Insert]	[Actual/ Good x100]	[Insert]
[Insert]	Q [insert] [Year]	[Threshold]	[Threshold]	[Threshold]	[Threshold]	[Insert]	[Actual/ Good x100]	[Insert]
[Insert]	Q [insert] [Year]	[Threshold]	[Threshold]	[Threshold]	[Threshold]	[Insert]	[Actual/ Good x100]	[Insert]
[Insert]	Q [insert] [Year]	[Threshold]	[Threshold]	[Threshold]	[Threshold]	[Insert]	[Actual/ Good x100]	[Insert]

- 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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 3
PERFORMANCE LEVELS

Schedule 3 (*Performance Levels*)

1. DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

“Available”	has the meaning given in Paragraph 10 of Annex 1 Part B of Annex 1;
“Bronze Site”	has the meaning given in Table 13 (Site Availability Requirement Levels);
“Business Hour”	an hour between 9am and 5pm on a Working Day
“DMMP”	has the meaning given in Paragraph 1.1(a) of Part B;
“Gold Site”	has the meaning given in Table 13 (Site Availability Requirement Levels);
“On Hold Time”	means the period of time that Resolution or fulfilment of Catalogue Item(s) is paused commencing from when the Authority or a Service Recipient receives a request from the Supplier for: (a) information without which diagnosis and Resolution of the Service Incident or Security Incident – or fulfilment of the Catalogue Items(s) – cannot progress; or (b) an End User to test and/or confirm whether the Service Incident or Security Incident has been Resolved or whether fulfilment of the Catalogue Item(s) has been completed correctly, and ending when the actions in (a) or (b) have been completed.
“Performance Monitoring Report”	has the meaning given in Paragraph 1.2 of Annex 1 Part B
“Performance Review Board”	the regular meetings between the Supplier and the Authority to manage and review the Supplier's

SCHEDULE 3 (Performance Levels)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

performance under this Contract, as further described in Paragraph 6.10 of Part B;

“Repeat KPI Failure”	has the meaning given in Paragraph 3.1 of Part A;
“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	the deadline for Resolution in accordance with the following paragraphs of Part B of Annex 1: – for Service Incidents, Paragraph 1.9; and – for Security Incidents, Paragraph 2.4.
“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;
“Satisfaction Survey”	has the meaning given in Paragraph 6.4 of Part B;
“Service Downtime”	any period of time during which the Fixed LAN, WLAN and/or the DMMP (as appropriate) is not Available;
“Service Hours”	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);
“Security Incident”	has the meaning given in Paragraph 2.1 of Part B of Annex 1;

SCHEDULE 3 (Performance Levels)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**“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;

“Silver Site”

has the meaning given in Table 13 (Site Availability Requirement Levels);

“VIP Site(s)”

has the meaning given in Paragraph 1.5 of Part B of Annex 1.

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

- 1.1 Annex 1 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) with effect from the following dates:
 - 1.2.1 the Performance Indicators set out in Table 1 and Table 3 of Part A of Annex 1 shall apply from the date on which Milestone 5 is Achieved;
 - 1.2.2 the Performance Indicators set out in Table 2 and Table 4 of Part A of Annex 1 shall apply from the date on which Milestone 8 is Achieved.
- 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 Paragraph 2.3.
- 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.

3. REPEAT KPI FAILURES AND RELATED KPI FAILURES**Repeat KPI Failures**

- 3.1 If a KPI Failure occurs in respect of the same Key Performance Indicator in any two consecutive Measurement Periods, the second and any subsequent such KPI Failure shall be a **"Repeat KPI Failure"**.

SCHEDULE 3 (Performance Levels)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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:

$$SP = P \times 2$$

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.

<i>Worked example for information only based on the following Service Points regime for KPI-01 – Incident Resolution Times: Severity 1 Incidents</i>		Service Points
Target Performance Level:	0 minutes late	0
Minor KPI Failure:	>1 minute; up to 2 hours late	22 SP, then 1 additional SP per 5 minutes
Serious KPI Failure:	>2 hours late; up to 4 hours late	46 SP, then 1 additional SP per 4 minutes
Severe KPI Failure:	>4 Hours late, Up to 10 hours late	76 SP, then 1 additional SP per 2 minutes
KPI Service Threshold:	>10 hours late	256 SP, then 1 additional SP per 2 minutes

Example 1:

If the Supplier resolves in 20 minutes which is between 1 minute and up to 2 hours in 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 an additional 1 Service Point for every 5 minutes late, therefore total Service Points = 22 + (20/5) = 26.

If, in the next Measurement Period, the Supplier resolves in 140 minutes which is between 120 minutes and up to 4 hours it will incur a Serious KPI Failure and accordingly accrue 46 Service Points and then an additional 1 Service Point for each 4 minutes late, therefore total Service Points = 46 +

SCHEDULE 3 (Performance Levels)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

(20/4) = 51. but as the failure is a Repeat KPI Failure, the Service Points will be $51 \times 2 = 102$ Service Points.

If, in the next Measurement Period, the Supplier resolves in 20 minutes which is between 1 minute and up to 2 hours, 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 an additional 1 Service Point for every 5 minutes late, therefore total Service Points = $22 + 20/5 = 24$, but as the failure is again a Repeat KPI Failure the Supplier will incur Service Points of $24 \times 2 = 48$.

Example 2:

If the Supplier resolves in 140 minutes which is between 120 minutes and up to 4 hours late it will incur a Serious KPI Failure and accordingly accrue 46 Service Points and then an additional 1 Service Point for each 4 minutes late, therefore total Service Points = $46 + 20/4 = 51$.

If, in the next Measurement Period, the Supplier resolves in 20 minutes which is between 1 minute and up to 2 hours, 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 an additional 1 Service Point for every 5 minutes late, therefore total Service Points = $22 + 20/5 = 26$, but as the failure is a Repeat KPI Failure the Supplier will incur Service Points of $26 \times 2 = 52$.

If, in the next Measurement Period, the Supplier resolves in 20 minutes which is between 1 minute and up to 2 hours, 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 an additional 1 Service Point for every 5 minutes late, therefore total Service Points = $22 + 20/5 = 26$, but as the failure is again a Repeat KPI Failure the Supplier will incur Service Points of $26 \times 2 = 52$.

3.3 Not used.

4. PERMITTED MAINTENANCE

4.1 The Supplier shall be allowed to book Service Downtime for Permitted Maintenance in any one Service Period 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.

SCHEDULE 3 (Performance Levels)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- 5.2 The Supplier shall use the Performance Monitoring Reports provided pursuant to Annex 1
- 5.3 Part B, among other things, to verify the calculation and accuracy of the Service Credits (if any) applicable to each Service Period.
- 5.4 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.
- 5.5 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.

Part B: Performance Monitoring

6. PERFORMANCE MONITORING AND PERFORMANCE REVIEW

- 6.1 The performance of the Supplier against each of the Performance Indicators shall be monitored and measured as follows:
- (a) Availability and Vulnerability Management shall be monitored and measured in the Device Management & Monitoring Platform (the “**DMMP**”) except for Availability and Vulnerability Management of the DMMP itself;
 - (b) the Parties shall agree how Availability and Vulnerability of the DMMP itself shall be monitored and measured during the Implementation Period in accordance with the Change Control Procedure;
 - (c) the Social Value PI shall be monitored and measured in accordance with the Social Value Delivery Plan; and
 - (d) all other Performance Indicators shall be monitored and measured in the ITSM Toolset in accordance with the Authority’s processes relating to the ITSM Toolset, unless otherwise agreed by the Authority.
- 6.2 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 6.6 (the “**Performance Monitoring Report**”).
- 6.3 Within ten (10) Working Days of the end of each Service Period, the Supplier shall, upon request from the Authority in accordance with Paragraph 6.7, provide a report to the Authority Representative which summarises the Supplier’s performance over the relevant Service Period as more particularly described in Paragraph 6.7 (the “**Balanced Scorecard Report**”).
- 6.4 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.
- 6.5 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 (each survey a “**Satisfaction Survey**”), and any results relevant to the Services will be summarised in the Performance Monitoring Report.

Performance Monitoring Report

- 6.6 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

- (a) for each Key Performance Indicator and Subsidiary Performance Indicator, the actual performance achieved over the Service Period;
- (b) a summary of all Performance Failures that occurred during the Service Period;
- (c) the performance level of each Performance Indicator as defined in Table 8, Table 9, Table 10, Table 11 and Table 12 in Paragraphs The Appendix1, 2 and 1 of Part 1 of Annex A (*i.e.* “Target Performance Level”, “Minor KPI Failure”, “Severe KPI Failure”, “KPI Service Threshold”, “Service Threshold”);
- (d) which Performance Failures remain outstanding and progress in resolving them;
- (e) 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;
- (f) for any Repeat KPI Failures, actions taken to resolve the underlying cause and prevent recurrence;
- (g) the number of Service Points awarded in respect of each KPI Failure;
- (h) the Service Credits to be applied, indicating the KPI Failure(s) to which the Service Credits relate;
- (i) any relevant matters arising from Satisfaction Surveys;
- (j) 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;

SCHEDULE 3 (Performance Levels)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (k) the conduct and performance of any agreed periodic tests that have occurred, such as the annual failover test of the Service Continuity Plan; and
- (l) relevant particulars of any aspects of the Supplier's performance which fail to meet the requirements of this Contract;
- (m) such other details and/or sections for Supplier input as the Authority may reasonably decide from time to time; and

Information in respect of previous Service Periods

- (n) for each Key Performance Indicator and Subsidiary Performance Indicator, the actual performance achieved over the previous 12 months;
- (o) a rolling total of the number of Performance Failures that have occurred over the past six Service Periods;
- (p) the amount of Service Credits that have been incurred by the Supplier over the past six Service Periods;
- (q) 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; and

Information in respect of the next Quarter

- (r) 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; and
- (s) at least quarterly, continuous service improvement opportunities in respect of performance achieved.

Balanced Scorecard Report

6.7 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 6.3 and 6.8, and until such notice is made the Supplier shall not be required to perform those requirements.

6.8 Upon request from the Authority in accordance with Paragraph 6.7, 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;

SCHEDULE 3 (Performance Levels)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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.
- 6.9 The Performance Monitoring Report – and, if requested by the Authority under Paragraph 6.7, the Balanced Scorecard Report – shall be reviewed and their contents agreed by the Parties at the next Performance Review Board held in accordance with Paragraph 6.10.
- 6.10 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 6.7, the Balanced Scorecard Reports (the **“Performance Review Board”**). The Performance Review Board shall (unless otherwise agreed):
- (a) take place within 5 Working Days of the updated 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.
- 6.11 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.
- 6.12 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 Paragraph 1.5 of Part E of Schedule 15 (*Charges and Invoicing*), must accompany the relevant invoice.
- ## 7. PERFORMANCE RECORDS
- 7.1 In addition to any other Management Information and record keeping requirements set out in this Contract, the Supplier shall keep appropriate

SCHEDULE 3 (Performance Levels)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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.

- 7.2 In addition to the requirement in Paragraph 7.1 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.
- 7.3 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.

8. PERFORMANCE VERIFICATION

- 8.1 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.

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 8 shall apply to all Operational Services.

Table 8 – KPIs for all Operational Services

No.	Key Performance Indicator title	Definition	Frequency of measurement	Performance levels	Service Points	Publishable Performance Information
KPI-01	Incident Resolution Times: Severity 1 Service Incidents & Severity 2 Service Incidents	See Paragraph 1.10 of Annex 1 Part B of this Annex	Monthly	See Paragraph 1.11 of Annex 1 Part B of this Annex	Paragraph 1.12 of Part B of this Annex and Table 8 describe the Service Points for this KPI and the methodology for calculating Service Points.	Yes

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

No.	Key Performance Indicator title	Definition	Frequency of measurement	Performance levels	Service Points	Publishable Performance Information
KPI-02	Incident Resolution Times: Severity 3 Service Incidents	See Paragraph 1.10 of Annex 1 Part B of this Annex	Monthly	See Paragraph 1.11 of Part B of this Annex	Paragraph 1.12 of Part B of this Annex and Table 8 describe the Service Points for this KPI and the methodology for calculating Service Points.	Yes
KPI-03	Security Incident Response Time: Severity 1, Severity 2 and Severity 3 Security Incidents	See Paragraph 2.2 of Annex 1 Part B of this Annex	Monthly	See Paragraph 2.6 of Annex 1 Part B of this Annex	Paragraph 2.7 of Part B of this Annex and Table 10 describe the Service Points for this KPI and the methodology for calculating Service Points.	No
KPI-04	Security Incident Resolution Time: Severity 1, Severity 2	See Paragraph 08 of Annex 1 Part B of this Annex	Monthly	See Paragraph 2.9 of Annex 1 Part B of this Annex	Paragraph 2.10 of Part B of this Annex and Table 12 describe the Service Points for this KPI and the methodology for calculating Service Points.	No

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

No.	Key Performance Indicator title	Definition	Frequency of measurement	Performance levels	Service Points	Publishable Performance Information
	and Severity 3 Security Incidents					
KPI-05	Change Management	See Paragraph 3.2 of Annex 1 Part B of this Annex	Monthly	Target Performance Level: 98% Minor KPI Failure: 97% - 97.99% Serious KPI Failure: 96.01% - 96.99% Severe KPI Failure: 95.01% - 96% KPI Service Threshold: Below 95.01%	Target Performance Level: 0 Minor KPI Failure: 10 <i>Then 1 SP per increment 0.1 %</i> Serious KPI Failure: 20 <i>Then 1 SP per 0.1 increment %</i> Severe KPI Failure: 30 <i>Then 1 SP per 0.1 increment %</i> KPI Service Threshold: 40 <i>Then 1 SP per 0.1 increment %</i>	Yes

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

No.	Key Performance Indicator title	Definition	Frequency of measurement	Performance levels	Service Points	Publishable Performance Information
KPI-06	Service Request Fulfilment	See Paragraph 4.1 of Annex 1 Part B of this Annex	Monthly	Target Performance Level: 98% Minor KPI Failure: 97.00% – 97.99% Serious KPI Failure: 96.00% – 96.99% Severe KPI Failure: 95.01% – 95.99% KPI Service Threshold: Below 95.01%	Target Performance Level: 0 Minor KPI Failure: 10 <i>Then 1 SP per 0.1 increment %</i> Serious KPI Failure: 20 <i>Then 1 SP per 0.1 increment %</i> Severe KPI Failure: 30 <i>Then 1 SP per 0.1 increment %</i> KPI Service Threshold: 40 <i>Then 1 SP per 0.1 increment %</i>	Yes

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

No.	Key Performance Indicator title	Definition	Frequency of measurement	Performance levels	Service Points	Publishable Performance Information
KPI-07	Knowledge Managment	See Paragraph 5.2 of Annex 1 Part B of this Annex	Monthly	Target Performance Level: 97% Minor KPI Failure: 95% - 96.99% Serious KPI Failure: 92% - 94.99% Severe KPI Failure: 90.01% - 91.99% KPI Service Threshold: Below 90.01%	Target Performance Level: 0 Minor KPI Failure: 10 <i>Then 1 SP per 0.1 increment %</i> Serious KPI Failure: 20 <i>Then 1 SP per 0.1 increment %</i> Severe KPI Failure: 30 <i>Then 1 SP per 0.1 increment %</i> KPI Service Threshold: 40 <i>Then 1 SP per 0.1 increment %</i>	Yes

1.2 The Key Performance Indicators in Table 9 shall apply to the Soft LAN Services.

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Table 9 - KPIs for Soft LAN Services

No.	Key Performance Indicator Title	Definition	Frequency of measurement	Performance levels	Service Points	Publishable Performance Information
KPI-08	Availability: DMMP	See Paragraph 11.2 of Annex 1 Part B of this Annex	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% KPI Service Threshold: Below 99%	1 Service Point for each 0.01% below the Target Performance Level	Yes
KPI-09	Site Availability: Fixed LAN Services	See Paragraphs 10 and 11.2 of Annex 1 Part B of this Annex	Monthly	See Paragraph 11.4 of Annex 1 Part B of this Annex	1 Service Point for each 0.01% below the Target Performance Level	Yes

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

No.	Key Performance Indicator Title	Definition	Frequency of measurement	Performance levels	Service Points	Publishable Performance Information
KPI-10	Site Availability: WLAN Services	See Paragraphs 10 and 11.2 of Annex 1 Part B of this Annex	Monthly	See Paragraph 11.4 of Annex 1 Part B of this Annex	1 Service Point for each 0.01% below the Target Performance Level	Yes

2 Subsidiary Performance Indicators

2.1 The Subsidiary PIs in Table 10 shall apply to all Operational Services and Social Value.

Table 10 - 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)	YES

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Performance levels	Publishable Performance Information
				PI Service Threshold: “Inadequate” (as defined in the SVDP) shall be considered below threshold	
SPI-02	Proposal Turnaround	See Paragraph 6 of Annex 1 Part B of this Annex	Monthly	Target Performance Level: 95% PI Service Threshold: Below 90%	YES
SPI-03	Change Success	See Paragraph 3.3 of Annex 1 Part B of this Annex	Monthly	Target Performance Level: 98% PI Service Threshold: Below 95%	YES
SPI-04	Catalogue Accuracy	See Paragraph 7 of Annex 1 Part B of this Annex	Monthly	Target Performance Level: 5 Working Days PI Service Threshold: 20 Working Days	YES

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Performance levels	Publishable Performance Information
SPI-05	CMDB Accuracy	See Paragraph 8 of Annex 1 Part B of this Annex	Quarterly	Target Performance Level: 99.6% PI Service Threshold: Below 98%	NO
SPI-06	Root Cause Analysis	See Paragraph 9 of Annex 1 Part B of this Annex	Monthly	Target Performance Level: 95% PI Service Threshold: Below 93%	YES
SPI-07	Aged Service Incident Management	See Paragraph 1.14 of Annex 1 Part B of this Annex	Monthly	Target Performance Level: 95% PI Service Threshold: Below 93%	YES

2.2 The Subsidiary Performance Indicator in Table 11 shall apply to the Soft LAN Services.

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Table 11 - Subsidiary PI for Soft LAN Services

No.	Subsidiary Performance Indicator Title	Definition	Frequency of measurement	Performance levels	Publishable Performance Information
SPI-08	Vulnerability Management	See Paragraph 12 of Annex 1 Part B of this Annex 1	Monthly	Target Performance Level: 95% PI Service Threshold: Below 90%	No
SPI-09	Capacity Management	See Paragraph 13 of Annex 1 Part B of this Annex 1	Monthly	Target Performance Level: no more than 1% of Resolved Service Incidents have a capacity-related Resolution code as recorded in the ITSM ToolsetPI Service Threshold: Below 4%	No

OPTIONAL SERVICES

The Key Performance Indicators and Subsidiary Performance Indicators that shall apply to the Optional Services are set out below:

1 Performance Indicators for Optional Services

Table 12 - PIs for Optional Services - Not used

No.	Performance Indicator Title	Definition	Frequency of Measurement	Performance Levels	Service Points	Publishable Performance Information

Annex 1

Part B: Definitions

1 INCIDENT RESOLUTION TIMES

1.1 Resolution Times for Severity 1 Service Incidents and Severity 2 Service Incidents shall be measured 24x7, excluding On Hold Time.

1.2 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 0800–21:30, then the clock stops measuring Resolution Time at 21:30 in the evening and restarts at 0800 the following day.

1.3 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 13:

Table 13 - Service Incident severity levels

Service Incident severity	Title (For information; used in Authority's incident management process.)	Description
1	Major incident	In relation to a Gold Site or a Silver Site, failure, or Unavailability, or reduction in performance or loss of functionality of all or part of the LAN 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: End Users performing mission-critical work at Gold/Silver Sites(s) cannot reliably connect to the WLAN or Prison-to-court video services unusable owing to QoS under-performance.
2	High	Failure, or Unavailability, or reduction in performance or loss of functionality of all or part of the LAN that results in significant business impact where there is no alternative way to work.

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

Service Incident severity	Title (For information; used in Authority's incident management process.)	Description
		For example: Fixed or Wireless LAN network performance issues affecting a large proportion of users.
3	Medium	Failure, or Unavailability, or reduction in performance or loss of functionality of all or part of the LAN and / or 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 LAN and / or Services. For example: a single End User is impacted by Unavailability, loss of functionality or a reduction in performance of all or part of the LAN and / or Services.
4	Low	Any other Service Incident that is none of the above and has no impact from an End User perspective but requires management. For example: An End User unable to print from a particular printer but has access to other printers.

and the expressions “**Severity 1 Service Incident**”, “**Severity 2 Service Incident**”, etc. shall be interpreted with reference to the Service Incident severities in Table 13.

- 1.4 Examples given in Table 13 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.
- 1.5 The Authority may by giving notice to the Supplier in writing from time to time within the Authority Site List:
 - (a) 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
 - (b) de-classify an Authority Site so that it is no longer designated as a VIP Site,

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

provided that the total number of VIP Sites at any time does not exceed 40 Authority Sites.

- 1.6 Notwithstanding Paragraph 1.3, 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.
- 1.7 For the avoidance of doubt, Paragraph 1.6 shall not affect the Service Incident severity level for the purposes of measuring the Key Performance Indicators.
- 1.8 For the purposes of this Paragraph 1, the following expressions shall have the meanings set opposite them below:

“Aged Service Incident”

A Service Incident without Resolution after twenty (20) Working Days from the date it was reported to the Supplier;

- 1.9 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.

For the avoidance of doubt, the two (2) hour Resolution Deadline for Severity 1 Service Incidents shall only apply to Service Incidents impacting one or more Gold Sites or Silver Sites. The maximum Severity Level for a Service Incident impacting one or more Bronze Sites will be a Severity 2 Service Incident.

- 1.10 “Incident Resolution Time” shall be measured:

- (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; and
- (b) for Severity 3 Service Incidents, 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.

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- 1.11 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 1.9, as shown in Table 14:

Table 14 - 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
Target Performance Level	0 minutes late	0 minutes late	98%
Minor KPI Failure	>1 minute late; up to 2 hours late	>1 minute late; up to 2 hours late	97.51% - 97.99%
Serious KPI Failure	>2 hours late; up to 4 hours late	>2 hours late; up to 8 hours late	97.01% - 97.50%
Severe KPI Failure	>4 hours late; up to 10 hours late	>8 hours late; up to 20 hours late	96.01% - 97%
KPI Service Threshold	>10 hours late	>20 hours	Below 96.01 %

- 1.12 Service Points (“**SP**”) for 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.

Table 15 - 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	1 SP
Serious KPI Failure	46 SP; then 1 additional SP per 4 minutes	40 SP; then 1 additional SP per 5 minutes	2 SP
Severe KPI Failure	76 SP; then 1 additional SP per 2 minutes	112 SP; then 1 additional SP per 5 minutes	3 SP
KPI Threshold	256 SP; then 1 additional SP per 2 minutes	256 SP; then 1 additional SP per 5 minutes	4 SP

1.13 Not used.

1.14 **“Aged 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.

2 SECURITY INCIDENT RESPONSE & RESOLUTION

2.1 For the purposes of this Paragraph 2, the following expressions shall have the meanings set opposite them below:

“Response Deadline” the deadline for Response in accordance with Paragraph 2.3

**ANNEX 1 (Key Performance Indicators and Subsidiary
Performance Indicators)**

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

“Response Time”	the period from the time that the Security Incident is reported to the Supplier to the point of personal acknowledgement on record by a member of the Supplier Personnel.
“Security Incident”	the act of breaching an explicit or implied security policy;
“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 agreed with the Authority in accordance with the Incident Management Process to investigate, diagnose, resolve, and prevent future occurrences of the Security Incident;
“Severity 1 Security Incident”	a Security Incident impacting one or more Gold Sites or Silver Sites 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

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

and/or affects the reputation of Government bodies and services; or

- (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.

2.2 For the avoidance of doubt, where a Security Incident is detected in relation to a Service Incident, 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.

2.3 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.

2.4 The Resolution Deadlines for Security Incidents shall be:

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- (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
- (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) hours;
 - for Severity 4 Security Incidents, 56 (fifty six) hours; or
- (c) as otherwise agreed with the Authority.

For the avoidance of doubt, the two (2) hour Resolution Deadline for Severity 1 Security Incidents shall only apply to Security Incidents affecting one or more Gold Sites or Silver Sites. The maximum Severity Level for a Security Incident affecting one or more Bronze Sites will be a Severity 2 Security Incident.

2.5 “**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.

2.6 Performance levels for Security Incident Response Time shall be measured in accordance with Table 16:

Table 16 - 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;	>4 hours late;	>8 Service Hours late;	N/A

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

	up to 3½ hours late	up to 7 hours late		
KPI Service Threshold	>3½ hours late	>7 hours late	N/A	N/A

2.7 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 Severe KPI Failure as shown in Table 16; 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 17.

Table 17 - 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	340 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	700 SP; then 4 SP per minute	630; then 2 SP per minute	220 SP; then 1 SP per 6 minutes	0 SP

- 2.8 “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.

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- 2.9 Performance levels for Security Incident Resolution Time shall be the number of minutes greater than the Resolution Deadline, as shown in Table 18, unless otherwise agreed by the Authority in respect of a Security Incident Resolution Plan:

Table 18 - 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
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
KPI Service Threshold	>12 hours late	>24 hours late	≥ 4 Working Days late

- 2.10 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 18) and (ii) at a rate of Service Points per minute indicated in Table 17 12, while Resolution Time is within the duration for the respective performance level (as shown in Table 18).

Table 19 - 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

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

Performance level	Severity 1 Security Incidents	Severity 2 Security Incidents	Severity 3 Security Incidents
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
KPI Threshold	SP; then 1 SP per 3 minutes	250 SP; then 1 SP per 6 minutes	250 SP; then 15 SP per Service Hour

3 SERVICE CHANGES

3.1 For the purposes of this Paragraph 3, the following expressions shall have the meanings set opposite them below:

“Uncontrolled 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.

3.2 **“Change Management”** shall be measured according to 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 Uncontrolled Changes within the relevant Service Period.

3.3 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.

3.4 **“Change Success”** shall be measured as Service Changes which meet the success criteria specified in the relevant authorised RFC, as a percentage of all Service Changes which were completed within the Service Period.

4 SERVICE REQUEST FULFILMENT

4.1 **“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 a percentage of all Service Requests which have Catalogue Items with fulfilment dates which are due to be completed within the Service Period in accordance with Schedule 22 (*Change Control Procedure, Service Requests & Projects*).

4.2 The measurement of time taken to fulfill Catalogue Item(s) shall exclude On Hold Time.

5 KNOWLEDGE MANAGEMENT

5.1 For the purposes of this Paragraph 5, the following expressions shall have the meanings set opposite them below:

“Current Record” Subject to Paragraph 5.4, 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 including a Knowledge Management Artefact 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

5.2 **“Knowledge Management”** shall measure completeness of the Knowledge Management Artefacts according to the following formula:

$$\text{Knowledge Management \%} = \frac{(K-D) \times 100}{K}$$

where:

K = total number of Knowledge Management Artefacts required in accordance with Schedule 24 (*Reports and Records Provisions*) (*Annex 3: Records to Upload To Virtual Library*), subject to Paragraph 5.3; and

D = total number of Knowledge Management Artefacts which are missing and/or not Current Records.

5.3 Where the Supplier has been relieved of responsibility to maintain any Records, in accordance with Paragraph 4.18 of Schedule 24, such Records

shall be excluded from the number of Knowledge Management Artefacts calculated for function *K* in the formula in Paragraph 5.2.

- 5.4 Notwithstanding the definition of Current Record in Paragraph 5.1, 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.

6 PROPOSAL TURNAROUND

- 6.1 **“Proposal Turnaround”** shall be measured as Project Proposals submitted within the time period in accordance with Paragraph 5.1 (*Project Proposals*) of Part B of Schedule 22 (*Change Control Procedure, Service Requests & Projects*) as a percentage of all agreed Project Requests which have been issued and are due to receive Project Proposals within the Service Period in accordance Schedule 22 (*Change Control Procedure, Service Requests & Projects*).
- 6.2 Project Requests that are withdrawn by the Authority before a Project Proposal has been provided by the Supplier shall be excluded from the measurement of Proposal Turnaround.

7 CATALOGUE ACCURACY

- 7.1 **“Catalogue Accuracy”** shall be measured per Catalogue Item, where an error or omission in the Product and Service Catalogue has been reported to the Supplier, from the date of such report to the date that such error or omission has been rectified to the satisfaction of the Authority.
- 7.2 The measurement in Paragraph 7.1 shall be in Working Days, excluding any Working Days where the Supplier has requested and is waiting:
- (a) for more than 5 Business Hours for information it has requested from the Authority and/or Service Recipients that is necessary to clarify a report and without which rectification of the error or omission cannot progress; or
 - (b) for an End User to check and/or confirm the error or omission has been rectified.

8 CMDB ACCURACY

- 8.1 **“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) Authority Assets from Authority Site(s) and using mandatory fields nominated by the Authority, and measure the accuracy and

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

completeness of the information held within the CMDB for those Authority Assets.

- (b) The Supplier shall not select the same sample of Authority Assets to be measured in two consecutive Measurement Periods, and the Supplier must sample at least ten percent (10%) of the volume of the CMDB in each Contract Year, following the Effective 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 Authority Assets correctly recorded in the CMDB in the Measurement Period; and

E is the number of Authority Assets excluded in accordance with Paragraph 8.2.

8.2 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.

9 ROOT CAUSE ANALYSIS

9.1 “Root Cause Analysis” shall be measured as the number of root cause analysis reports provided by Supplier in accordance with the Authority’s problem management process, as a percentage of all such root cause analysis reports due in the Service Period.

10 AVAILABLE

10.1 The Fixed LAN and the WLAN at an Authority Site shall be Available when:

- (a) End Users are able to access and utilise all the functions of the Fixed LAN or the WLAN (as the case may be) at that Authority Site; and
- (b) the Vulnerability Management Performance Indicator (SPI-08) is above the relevant PI Service Threshold.

10.2 The DMMP shall be Available when:

- (a) End Users are able to access and utilise all the functions of the DMMP; and
- (b) the DMPP is able to process the Authority Data and to provide any required reports within the timescales set out in the Services Description,

as measured on a 24 x 7 basis.

11 AVAILABILITY

- 11.1 “Table 13 sets out the required level of Availability for the Fixed LAN and the WLAN specified by the Authority in the Authority Site List according to mission-criticality of functions performed at the relevant Authority Site:

Table 20 - Site Availability Requirement Levels

Required Availability	Minimum specification for Authority Site
99.99% - Gold Site	Has resilient core switches and core and access layers: Definition of Gold Site : means an Authority Site which is specified as being a Gold Site in the Authority Site List and in the reasonable opinion of the Authority, has resilient core switches and core and access layers. Gold Sites typically have greater than 20 switch deployments
99.95% - Silver Site	Has resilient core switches and core and access layers Definition of Silver Site : means an Authority Site which is specified as being a Silver Site in the Authority Site List and in the reasonable opinion of the Authority, has resilient core switches and core and access layers.
99.90% - Bronze Site	Has access layer architecture Definition of 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 no resilience (single point of failure) and an access layer only architecture.

- 11.2 “**Availability**” shall be measured for each of the following:

- (a) the DMMP;

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

(b) Fixed LAN at each Authority Site; and

(c) WLAN at each Authority Site;

as a percentage of the total time in a Service Period, 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.

11.3 When calculating Availability in accordance with Paragraph 11.2:

- (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.

11.4 Availability performance levels for Fixed LAN Services and Wireless LAN Services shall be as follows:

Site Availability Requirement:	99.99% - Gold Site	99.95% - Silver Site	99.90% - Bronze Site
Target Performance Level	99.99%	99.95%	99.90%
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%

ANNEX 1 (Key Performance Indicators and Subsidiary Performance Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

KPI Service Threshold	Below 99%	Below 98%	Below 98%

11.5 In respect of “Availability”, 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.

11.6 If Availability cannot be measured in accordance with this Schedule 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 Key Performance Indicators;
- (b) the Authority shall seek to infer Availability status from data sources available, including information provided by the Supplier in accordance with Sub-paragraph 11.6(a) and ITSM Toolset records (e.g., Service Incident logs); and
- (c) if Availability cannot be ascertained or inferred in accordance with 11.6(a) and 11.6(b) of this Paragraph, the Performance Level achieved for the relevant Authority Site shall be a Serious KPI Failure.

12 VULNERABILITY MANAGEMENT

12.1 “**Vulnerability Management**” shall be measured as the percentage of Devices:

- (a) with all security patches applied in accordance with Paragraph 9.3 of the Baseline Security Requirements;
- (b) where the version of software on the Device is up to date in accordance with the requirements of the Security Management Plan and Paragraph 9.5 of the Baseline Security Requirements; and
- (c) with all relevant Remediation Action Plans successfully implemented in accordance with Paragraph 9.4 (c) of Schedule 5 (Security Management).

12.2 Further detail of the methodology for the calculation in accordance with Paragraph 12.1 may be specified in the Security Management Plan.

13 CAPACITY MANAGEMENT

13.1 **“Capacity Management”** shall be measured as the percentage of Resolved Service Incidents in a Service Period with a capacity-related Resolution code as recorded in the ITSM Toolset.

13.2 When calculating Capacity Management in accordance with Paragraph 13.1, 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 forecast End User demand that exceeds pre-agreed thresholds.

SCHEDULE 4

STANDARDS

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, 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.

- 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:

SCHEDULE 4 (Standards)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (a) ITIL v3, as a minimum;
- (b) ISO/IEC 20000-1 2018 “Information technology — Service management – Part 1”;
- (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

SCHEDULE 4 (Standards)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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.

- 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
2	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
3	MoJ Cyber and Technical Security Guidance as documented at: https://security-guidance.service.justice.gov.uk
4	NCSC Guidance as documented at: https://www.ncsc.gov.uk/section/advice-guidance/all-topics
5	NCSC Cyber Assessment Framework as documented at: https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework
6	MoJ ICT Physical Infrastructure Standards v3.4
7	MoJ Comms Room Protocols
8	MoJ Project Delivery Standards
9	ISO/IEC 27001 – Information security, cybersecurity and privacy protection
10	ISO/IEC 27002 – Code of practice for information security management
13	HMG Functional Standard GovS 007: Security Government Functional Standard GovS 007: Security - GOV.UK (www.gov.uk);

11. INCOME SECURITY

- 11.1 The Supplier shall:

SCHEDULE 4 (Standards)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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.

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:

SCHEDULE 4 (Standards)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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
2	Change and Evaluation Management
3	Continual Service Improvement
4	Demand Management
5	Event Management
6	Incident Management
7	Knowledge Management
8	License Management and Compliance
9	Problem Management
10	Release and Deployment Management
11	Request Fulfilment
12	Service Asset and Configuration Management

No.	Process
13	Service Catalogue Management
14	Service Level Management
15	Service Design
16	Service Transition
17	Availability Management
18	IT Service Continuity Management
19	Risk Management
20	Supplier Management
21	Major Incident Management
22	Escalation Management
23	Complaint Management
24	Transition Framework

- 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 (Service 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 (Service 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 (Service 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).

ANNEX 1: SUSTAINABILITY

1 DEFINITIONS

1.1 In this Annex, the following definitions shall apply:

“Prohibited Items”	means those items which are not permissible under this Contract as set out at Table A of this Annex
“Sustainability Reports”	written reports to be completed by the Supplier containing the information outlined in Table C of this Annex
“Waste Hierarchy”	means prioritisation of waste management in the following order of preference as set out in the Waste (England and Wales) Regulation 2011: (c) Prevention; (d) Preparing for re-use; (e) Recycling; (f) Other Recovery; and (g) 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,

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:
- 3.3.1 demonstrate low carbon resource efficiency, including minimising the use of resources and responding promptly to the Authority's reasonable questions;
 - 3.3.2 prioritise waste management in accordance with the Waste Hierarchy as set out in Law;
 - 3.3.3 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;
 - 3.3.4 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;
 - 3.3.5 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 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;

- 3.3.6 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
 - 3.3.7 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.
- 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 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;
 - 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:

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.

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: <http://www.rohs.gov.uk/>

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:

<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/779660/20190220-Supplier_Code_of_Conduct.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 The Appendix2.1, The Appendix3.1 to The Appendix3.6, The Appendix5.1 and The Appendix6 of this Annex within fourteen (14) days of such request; and
 - 7.1.2 With Paragraphs The Appendix2.2, The Appendix2.3 and 3.7 to 3.12 of this Annex 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 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.

TABLE A – PROHIBITED ITEMS

The Supplier shall ensure that all Supplier Personnel comply with the prohibitions under this Table A when carrying out any installation, maintenance and/or repair services.	
The following consumer single use plastics are Prohibited Items:	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 d. Non-recyclable plastic stationary
	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, consumer single use plastics are Prohibited Items: This list is not limited to the current items or is indeed final, future care will be required for new plastics that can be added.
Project specific Prohibitions	As per above Prohibited Items

TABLE B – NOT USED

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	On the anniversary of the Effective Date

ANNEX 1: (Sustainability)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	employed by the Supplier in response to those risks.	
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 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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 5
SECURITY MANAGEMENT

1. Definitions and precedence**1.1 In this Schedule:**

“Anti-Malicious Software”	means software that scans for and identifies possible Malicious Software in the IT Environment;
“Breach of Security”	means an event that results, or could result, in: (a) any unauthorised access to or use of the Authority Data, the Services, the Core Information Management System, and/or the Wider Information Management System; and/or (b) the loss, corruption and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including any copies of such information or data, used by the Authority and/or the Supplier or any Sub-contractor in connection with this Contract;
“Certification Requirements”	means the information security requirements set out in Paragraph 8;
“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 9.1;
"Core Information Management System"	means those parts of the Wider Information Management System that that the Authority has determined in accordance with Paragraph 4.2 shall be subject to Security Assurance;
“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;

“Incident Management Process”	means the process which the Supplier shall implement immediately after it becomes aware of a Breach of Security which is intended to restore normal operations as quickly as possible, minimising any adverse impact on the Authority Data, the Authority, the Services and/or users of the Services and which shall be prepared by the Supplier in accordance with Paragraph 7 using the template set out in Annex 3;
“Information Assurance Assessment”	means the set of policies, procedures, systems and processes which the Supplier shall implement, maintain and update in accordance with Paragraph 5.4 in order to manage, mitigate and, where possible, avoid information security risks including cyber-attacks, hacks, data leaks, Personal Data Breaches and/or theft and which shall be prepared by the Supplier using the template set out in Annex 3;
“Information Security Approval Statement”	means a notice issued by the Authority which sets out the information risks which the Supplier has identified as being associated with using the Core Information Management System and confirms that: (a) the Authority is satisfied that the identified risks have been adequately and appropriately addressed; (b) the Authority has accepted the residual risks; and the Supplier may use the Core Information Management System to Process Authority Data;
“IT Health Check”	has the meaning given in Paragraph 9.1(a);
“LAN Software”	means the software (including firmware) installed on Devices, and the application(s) which form the DMMP;
“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 9.4(c)(i);

**“Required
Changes
Register”**

means the register within the Security Management Plan which is to be maintained and updated by the Supplier and which shall record each of the changes that the Supplier shall make 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 7.14 together with the date by which such change shall be implemented and the date on which such change was implemented;

**"Residual Risk
Statement"**

means a notice issued by the Authority which sets out the information risks associated with using the 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;

**"Risk
Management
Rejection Notice"**

has the meaning given in Paragraph 7.8(b);

**“Security
Assurance”**

has the meaning given in Paragraph 7.1;

**“Security
Management
Plan”**

means the document prepared by the Supplier using the template in Annex 3, comprising the artefacts listed in Paragraph 6.4;

"Security Test"

has the meaning given in Paragraph 9.2;

**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;

"Sub-contractor Security Requirements"

means those requirements set out in Annex 2; and

"Wider Information Management System"

means

(a) any:

- (i) information assets,
- (ii) IT systems,
- (iii) IT services; or
- (iv) Sites

that the Supplier or any Sub-contractor will use and/or support under the Services to Process, or support the Processing of, Authority Data and provide, or support the provision of, the Services; and

(b) the associated information management system, including all relevant:

- (i) organisational structure diagrams,
- (ii) controls,
- (iii) policies,
- (iv) practices,
- (v) procedures,
- (vi) processes; and
- (vii) resources.

1.2 If there is any conflict between any of the following, then the conflict shall be resolved in accordance with the following order of precedence:

- (a) this Schedule 5 (Security Management);
- (b) Annex 1 (Baseline Security Requirements);
- (c) Annex 2 (Security Requirements for Sub-Contractors);
- (d) any guidance issued by the NCSC;

unless expressly stated otherwise in Annexes 1 and/or 2.

2. Introduction

In place of accreditation, the Authority operates an integrated through-life security assurance process with Senior Information Risk Owners and Service Owners, that is equitable to the former accreditation process, i.e., the Services being implemented must be fully risk assessed from technical and non-technical perspectives and adhere to Authority security policies; this will include necessary technical testing and approvals. Any solution provided to the Authority will require to be assured in line with the NCSC Cyber Assessment Framework (CAF) <https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance>

2.1 This schedule sets out:

- (a) 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 Information Management System;
- (b) the process which shall apply to the Security Assurance of the Core Information Management System in Paragraph 7;
- (c) the Certification Requirements applicable to the Supplier and each of those Sub-contractors which Processes Authority Data in Paragraph 8;
- (d) the Certification Requirements applicable to the Wider Information Management System in Paragraph 8;
- (e) the Baseline Security Requirements in Annex 1, with which the Supplier must comply;
- (f) the Security Tests which the Supplier shall conduct or that the Authority may require to be conducted during the Term, in Paragraph 9;
- (g) the obligations on the Supplier to prevent the introduction of Malicious Software into the Core Information Management System and to scan for, contain the spread of, and minimise the impact of Malicious Software as set out in Paragraphs 11 and 11;
- (h) the Supplier's obligations 14 to:
 - (i) return or destroy Authority Data on the expiry or earlier termination of this Contract detailed in paragraph 14; and
 - (ii) report Breaches of Security to the Authority as detailed in Paragraph 13.

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:
- (a) the Sites;
 - (b) the IT Environment;
 - (c) the Core Information Management System; and
 - (d) the Services.
- 3.2 Notwithstanding the involvement of the Authority in assessing the arrangements which the Supplier implements to ensure the security of the Authority Data and the Core Information Management System, the Supplier shall be, and shall remain, responsible for:
- (a) 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
 - (b) the security of the Core Information Management System.
- 3.3 The Supplier shall:
- (a) comply with the security requirements in Annex 1; and
 - (b) ensure that each Sub-contractor that Processes Authority Data complies with the Sub-contractor Security Requirements in Annex 2.
- 3.4 The Supplier shall provide the Authority with access to Supplier Personnel responsible for information assurance to facilitate the Authority's assessment of the Supplier's compliance with its obligations set out in this Schedule at reasonable times on reasonable notice.

4. Core and Wider Information Management Systems

- 4.1 The information management systems in scope of this Schedule 5 comprise the Core Information Management System (which shall include the LAN and the DMMP) and the Wider Information Management System.
- 4.2 The Authority shall be responsible for determining the boundary between the Core Information Management System and the Wider Information Management System. In order to enable the Authority to make such determination, the Supplier shall within 5 Working Days of the Effective Date provide the Authority 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 its decision regarding the component parts of the Core Information Management System and its boundary with the Wider Information Management System.
- 4.4 The Supplier shall reproduce the Authority's decision as a diagram documenting the Core Information Management System, the Wider Information Management system and the boundary between the two. This diagram shall form part of the Security Management Plan.
- 4.5 Any proposed change to the component parts of the Core Information Management System or the boundary between the Core Information Management System and the Wider Information Management System shall be notified and processed in accordance with the Change Control Procedure and/or Change and Evaluation Management.

5. Statement of Information Risk Appetite and Baseline Security Requirements

- 5.1 The Authority may, at any time, provide the Supplier with a statement of information risk appetite for the IT Environment and the Services (the **"Statement of Information Risk Appetite"**).
- 5.2 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 lead to the Supplier incurring additional costs, such costs shall be agreed under the Change Control Procedure.
- 5.3 The Baseline Security Requirements are set out in Annex 1.
- 5.4 The system(s) in scope of the Baseline Security Requirements shall be the Core Information Management System, unless otherwise stated or unless the context otherwise requires.

6. Information Security Approval Statement and Security Management Plan

- 6.1 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 the Effective Date.
- 6.2 The Supplier (and the Sub-contractors) may not use the Core Information Management System or the Wider Information Management System to Process Authority Data unless and until:
 - (a) the Supplier has procured the conduct of an IT Health Check of the relevant components Supplier System that are associated with the

delivery of the Services by a CHECK Service Provider in accordance with Paragraph 9.1; and

- (b) the Authority has issued the Supplier with a Residual Risk Statement in accordance with Paragraph 7.8;

except as otherwise agreed by the Authority.

6.3 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Schedule and the Contract in order to ensure the security of the Authority Data and the Core Information Management System.

6.4 The Supplier shall prepare and submit to the Authority, for review within 40 Working Days of the Effective Date, its proposed Security Management Plan, which shall comprise:

- (a) the Information Assurance Assessment;
- (b) the Required Changes Register;
- (c) the Incident Management Process; and
- (d) the risk assessment and Risk Treatment Plan.

6.5 The Authority shall review the Supplier's proposed Security Management Plan as soon as possible and, in any event within 20 Working Days of receipt and shall either issue the Supplier with a Residual Risk Statement or a Risk Management Rejection Notice in accordance with Paragraph 7.9

6.6 The Authority may require, and the Supplier shall provide the Authority and its authorised representatives with:

- (a) access to the Supplier Personnel;
- (b) access to the Core Information Management System to audit the Supplier and its Sub-contractors' compliance with this Contract; and
- (c) such other information and/or documentation that the Authority or its authorised representatives may reasonably require,

to assist the Authority to establish whether the arrangements which the Supplier and its Sub-contractors have implemented in order to ensure the security of the Authority Data and the Core Information Management System are consistent with the representations in the Security Management Plan. The Supplier shall provide the access required by the Authority in accordance with this Paragraph within 10 Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Authority with the access that it requires as soon as practicable, and in any case no longer than 24 hours of receipt of such request.

7. Assurance of the Core Information Management System

- 7.1 The Core Information Management System shall be subject to an integrated, through-life process which is transparent, auditable and consistently applied in order to safeguard Authority Data, in accordance with this Paragraph 7 (**"Security Assurance"**).
- 7.2 The Supplier acknowledges that the purpose of Security Assurance is to ensure that:
- (a) the Security Management Plan accurately represents the Core Information Management System;
 - (b) the Authority is given sufficient confidence that the Core Information Management System will meet the requirements of the Baseline Security Requirements and the Statement of Risk Appetite (if issued);
 - (c) the residual risks of the Core Information Management System are no greater than those provided for in the Baseline Security Requirements and the Statement of Risk Appetite (if issued); and
 - (d) the Parties have confidence that the Core Information Management System is secure, compliant with relevant regulations and the Standards and meets the relevant security objectives, maintaining the confidentiality, integrity and availability of the Core Information Management System.
- 7.3 The Security Assurance approvals shall be performed by the Authority or by representatives appointed by the Authority.
- 7.4 In addition to any obligations imposed by Schedule 13 (*Implementation Plan*) or Schedule 14 (*Testing Procedures*) the Supplier must ensure that its Detailed Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Schedule 5 (*Security Management*), including any requirements imposed on Sub-contractors by Annex 2.
- 7.5 By the date specified in the Implementation Plan, the Supplier shall prepare and submit to the Authority the risk management documentation for the Core Information Management System, which shall be subject to approval by the Authority in accordance with Paragraph 5.4.
- 7.6 The Security Management Plan shall be structured in accordance with the template as set out in Annex 3 and include:
- (a) an assurance plan, which shall include:
 - (i) the dates on which each subsequent iteration of the Security Management Plan will be delivered to the Authority for review and staged approval; and

- (ii) the date by which the Supplier is required to have received a Residual Risk Statement from the Authority together with details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Authority Responsibilities which must be completed in order for the Supplier to receive a Residual Risk Statement pursuant to Paragraph 7.8;
 - (b) a formal risk assessment of the Core Information Management System and a Risk Treatment Plan for the Core Information Management System;
 - (c) a completed ISO/IEC 27001 (at least ISO/IEC 27001:2013) Statement of Applicability for the Wider Information Management System; the process for managing any security risks from Sub-contractors and third parties authorised by the Authority with access to the IT Environment, processes associated with the delivery of the Services, the Authority Premises, the Sites, the Supplier 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 Services;
 - (d) unless such requirement is waived by the Authority, proposed controls that will be implemented in respect of all aspects of the IT Environment and the Services and all processes associated with the delivery of the Services, including the Authority Premises, the Sites, the Supplier 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 Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;
 - (e) the Required Changes Register;
 - (f) evidence that the Supplier and each applicable Sub-contractor is compliant with the Certification Requirements; and
 - (g) the diagram documenting the Core Information Management System, the Wider Information Management System and the boundary between them, as set out in Paragraph 4.2.
- 7.7 To facilitate Security Assurance of the Core Information Management System, the Supplier shall provide the Authority and its authorised representatives with:

SCHEDULE 5 (Security Management)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (a) access to the Sites, ICT information assets and ICT systems within the Core Information Management System on request or in accordance with the Security Management Plan; and
 - (b) such other information and/or documentation that the Authority or its authorised representatives may reasonably require, to enable the Authority to establish that the Core Information Management System is compliant with the Security Management Plan.
- 7.8 The Authority shall review the Security Management Plan and issue to the Supplier either:
 - (a) 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
 - (b) a rejection notice stating that the Authority considers that the identified risks to the Core Information Management System have not been adequately or appropriately addressed, or the residual risks to the Core Information Management System have not been reduced to the level anticipated by the Statement of Information Risk Appetite (if the Statement of Information Risk Appetite has been provided in accordance with Paragraph 5.1), and the reasons why ("**Risk Management Rejection Notice**").
- 7.9 If the Authority issues a Risk Management Rejection Notice, the Supplier shall, within 20 Working Days of the date of the Risk Management Rejection Notice:
 - (a) address all of the issues raised by the Authority in such notice; and
 - (b) update and re-submit the Security Management Plan, as appropriate.
- 7.10 If the Authority issues a two or more Risk Management Rejection Notices, the failure to receive a Residual Risk Statement shall constitute a material Default and the Authority may by terminate this Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 31.1(b).
- 7.11 Subject to Paragraph 7.9, the process set out in Paragraphs 7.6 to 7.8 shall be repeated until such time as the Authority issues a Residual Risk Statement to the Supplier or terminates this Contract.
- 7.12 The Supplier shall not use the Core Information Management System to Process Authority Data before receiving a Residual Risk Statement, except as otherwise permitted by the Authority in writing.

SCHEDULE 5 (Security Management)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 7.13 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 7.
- 7.14 The Supplier shall notify the Authority as soon as practicable, and in any case within 48 hours after becoming aware of:
- (a) a significant change, or a significant planned change, to the components or architecture of the Core Information Management System;
 - (b) a new risk or vulnerability is identified to the components or architecture of the Core Information Management System;
 - (c) a vulnerability to the components or architecture of the Service which is classified 'Medium', 'High', 'Critical' or 'Important' in accordance with the classification methodology set out in Paragraph 9.2 of Annex 1 to this Schedule;
 - (d) a change in the threat profile;
 - (e) a Sub-contractor failure to comply with the Core Information Management System code of connection (if relevant);
 - (f) a significant change to any risk component;
 - (g) a significant change in the quantity of Personal Data held within the Core Information Management System;
 - (h) 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 Contract;
 - (i) a proposal to change any of the Sites from which any part of the Services are provided; and
 - (j) an ISO/IEC 27001 (at least ISO/IEC 27001:2013) audit report produced in connection with the Certification Requirements indicates significant concerns.
- 7.15 The Supplier shall update the Required Changes Register and provide the updated Required Changes Register to the Authority for review and approval within 10 Working Days after the initial notification under Paragraph 7.14 or such other timescale as may be agreed with the Authority.
- 7.16 The Supplier shall conduct a review of any threats, risks and vulnerabilities to the Core Information Management System when a significant change to the components or architecture of the Core Information Management System is planned (or has otherwise occurred), and shall provide a report of such

threats, risks and vulnerabilities to the Authority within one (1) month of the significant change.

- 7.17 If the Supplier fails to implement a change set out in the Required Changes Register by the date agreed with the Authority, such failure shall constitute a material Default and the Supplier shall:
- (a) immediately cease using the 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
 - (b) where such Default is capable of remedy, the Supplier shall remedy such Default within the timescales set by the Authority and, should the Supplier fail to remedy the Default within such timescales, the Authority may terminate this Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 31.1(b).
- 7.18 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.
- 7.19 The Supplier shall be solely responsible for the costs associated with developing and updating the Security Management Plan and carrying out any remedial action (e.g. to implement a change, including any change to the Core Information Management System) required by the Authority as part of the Security Assurance process.

8. Certification Requirements

- 8.1 The Supplier shall be certified as compliant with:

- (a) ISO/IEC 27001 (at least ISO/IEC 27001:2013) by a UK Accreditation Service-approved certification body or alternatively, is included within the scope of an existing ISO/IEC 27001 certification providing this covers all Services relevant to the Contract, and;
- (b) Cyber Essentials PLUS,

and shall provide the Authority with a copy of each such certificate of compliance before the Supplier shall be permitted to receive, store or Process Authority Data.

8.2 The Supplier shall ensure that each Sub-contractor is certified as compliant with:

- (a) ISO/IEC 27001 (at least ISO/IEC 27001:2013) by a UK Accreditation Service-approved certification body; and
- (b) Cyber Essentials PLUS,

and shall provide the Authority with a copy of each such certificate of compliance before the Sub-contractor shall be permitted to receive, store or Process Authority Data.

8.3 The Supplier shall ensure that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data:

- (a) securely destroys Authority Data only on Sites which are included within the scope of an existing ISO/IEC 27001 certification;
- (b) satisfies the Authority that its data destruction/deletion practices comply with UK GDPR requirements and follow all relevant NCSC guidance; and
- (c) maintains an asset register of all Authority supplied information, data and equipment to ensure Authority Assets are returned and/or deleted.

8.4 The Supplier shall provide the Authority with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph 8, before the Supplier or the relevant Sub-contractor (as applicable) shall be permitted to carry out the secure destruction of any Authority Data.

8.5 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier or any Sub-contractor ceases to be compliant with the Certification Requirements and, on request from the Authority, shall or shall procure that the relevant Sub-contractor shall:

- (a) immediately cease Processing the Authority Data; and
- (b) promptly return, destroy and/or erase the Authority Data in accordance with the requirements set out in Annexes 1 and 2.

8.6 The Authority may agree to exempt, in whole or part, the Supplier or any Sub-contractor from the requirements of this Paragraph 8. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Management Plan.

9. Security Testing

9.1 The Supplier shall, upon agreement and approval with the Authority:

SCHEDULE 5 (Security Management)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (a) procure testing of the Core Information Management System by a CHECK Service Provider ("**IT Health Check**"), at its own cost and expense; and
- (b) conduct such other security tests as may be required by the Authority acting reasonably and upon reasonable notice as agreed by the Authority.

9.2 The Supplier shall:

- (a) except as otherwise agreed by the Authority, complete all of the security tests required by Paragraph 9.1 before:
 - (i) the Supplier submits the Security Management Plan to the Authority for review in accordance with Paragraph 6; and
 - (ii) the Supplier is given permission by the Authority to Process or manage any Authority Data;
- (b) repeat the IT Health Check not less than once every 12 months during the Term and submit the results of each such test to the Authority for review in accordance with Paragraph 9.4;
- (c) conduct vulnerability scanning and assessments of the Core Information Management System on a monthly basis as agreed with the Authority;
- (d) 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
- (e) conduct such other tests as are required by:
 - (i) any Remediation Action Plans;
 - (ii) the ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification requirements;
 - (iii) the Security Management Plan; and
 - (iv) 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**").

SCHEDULE 5 (Security Management)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

9.3 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 within 10 Working Days, after completion of each Security Test.

9.4 In relation to each IT Health Check, the Supplier shall:

- (a) agree with the Authority the aim and scope of the IT Health Check;
- (b) promptly, and no later than 10 Working Days, following the receipt of each IT Health Check report, provide the Authority with a copy of the full IT Health Check report;
- (c) in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:
 - (i) 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:
 - (A) how the vulnerability will be remedied;
 - (B) unless otherwise agreed in writing between the Parties, the date by which the vulnerability will be remedied, which must be:
 - (1) 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";
 - (2) 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"; and
 - (3) within seven (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"; and
 - (C) 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;
 - (ii) comply with the Remediation Action Plan; and
 - (iii) conduct such further tests on the Core Information Management System as are required by the Remediation

Action Plan to confirm that the Remediation Action Plan has been complied with.

9.5 The Supplier shall ensure that any testing which could adversely affect the IT Environment 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 tests shall be agreed in advance with the Authority.

9.6 If any testing conducted by or on behalf of the Supplier identifies a new risk, new threat, vulnerability or exploitation technique that has the potential to affect the security of the Core Information Management System, the Supplier shall promptly, and no later than 2 working days, provide the Authority with a copy of the test report as soon as possible after becoming aware of such risk, threat, vulnerability or exploitation technique, and;

(a) propose interim mitigation measures to vulnerabilities in the Core Information Management System known to be exploitable where a security patch is not immediately available; and

(b) where and to the extent applicable, remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the IT Environment) within the timescales set out in the test report or such other timescales as may be agreed with the Authority.

9.7 The Supplier shall conduct such further tests as may be required by the Authority from time to time to demonstrate compliance with its obligations set out this Schedule and the Contract. Any such further tests shall be agreed by the Parties in accordance with the Change Control Procedure.

9.8 The Supplier shall notify the Authority immediately if it fails to, or believes that it will not, mitigate the vulnerability within the timescales set out in Paragraph 9.4.

10. Security Monitoring and Reporting

10.1 The Supplier shall:

(a) monitor the delivery of assurance activities;

(b) maintain and update the Security Management Plan in accordance with Paragraph 7;

(c) agree a document which presents the residual security risks to inform the Authority's decision to give approval to the Supplier to Process and transit the Authority Data;

(d) monitor security risk impacting upon the operation of the LAN and/or the Services in accordance with Annex 1, Paragraph 7;

- (e) report Breaches of Security in accordance with the Incident Management Process;
- (f) within 20 Working Days of the Effective Date, agree with the Authority the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Authority.

11. Malicious Software

11.1 Except where otherwise agreed by the Authority, the Supplier shall:

- 11.1.1 install and maintain Anti-Malicious Software or procure that Anti-Malicious Software is installed and maintained on any part of the Wider Information Management System which may Process Authority Data;
- 11.1.2 ensure that such Anti-Malicious Software is configured to perform automatic software and definition updates and regular scans of the Wider Information Management System to check for and prevent the introduction of Malicious Software;
- 11.1.3 and if Malicious Software has been introduced into the Wider Information Management System, identify and contain the spread of, and minimise the impact of, the Malicious Software.

11.2 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 LAN and/or Services to the desired operating efficiency.

11.3 Any cost arising out of the actions of the parties taken in compliance with the provisions of Paragraph 11.2 shall be borne by the parties as follows:

- (a) by the Supplier where the Malicious Software originates from:
 - (i) the Supplier Software;
 - (ii) the Third Party Software supplied by the Supplier; or
 - (iii) the Authority Data whilst the Authority Data is or was under the control of the Supplier,

unless, in the case of the Authority Data only, 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

- (b) by the Authority, in any other circumstance.

12. Vulnerabilities and Corrective Action

- 12.1 The Authority and the Supplier acknowledge that vulnerabilities in the Core Information Management System may be discovered on an ongoing basis, which unless mitigated will present an unacceptable risk to the Authority Data.
- 12.2 The severity of vulnerabilities for LAN Software, Supplier COTS Software and Third Party COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the Security Management Plan and using the appropriate vulnerability scoring systems including:
- (a) 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
 - (b) Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.
- 12.3 Subject to Paragraph 12.4, the Supplier shall procure the application of security patches to vulnerabilities in the Core Information Management System within:
- (a) seven (7) days after the public release of patches for those vulnerabilities categorised as 'Critical';
 - (b) thirty (30) days after the public release of patches for those vulnerabilities categorised as 'Important'; and
 - (c) sixty (60) days after the public release of patches for those vulnerabilities categorised as 'Moderate' or 'Low'.
- 12.4 The timescales for applying patches to vulnerabilities in the Core Information Management System set out in Paragraph 12.3 shall be extended where:
- (a) 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 13.3 if the vulnerability becomes exploitable within the context of the Services;
 - (b) 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 five 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or

- (c) 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.

12.5 The Security Management Plan shall include provisions for major version upgrades of the LAN Software, all Supplier COTS Software and Third Party COTS Software to be kept up to date such that all Supplier COTS Software and Third Party COTS Software are always with support throughout the Term unless otherwise agreed by the Authority in writing.

12.6 The Supplier shall:

- (a) implement a mechanism for receiving, analysing and acting upon threat information supplied by NCSC, or any other competent Central Government Body;
- (b) promptly notify NCSC of any actual or sustained attempted Breach of Security;
- (c) ensure that the Core Information Management System is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;
- (d) ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Core Information Management System by actively monitoring the threat landscape during the Term;
- (e) pro-actively scan the Core Information Management System for vulnerable components and address discovered vulnerabilities through the processes described in the Security Management Plan;
- (f) from the date specified in the Security Management Plan and within 5 Working Days of the end of each subsequent month during the Term, provide the Authority with a written report which details both patched and outstanding vulnerabilities in the Core Information Management System, the elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report and any failure to comply with the timescales set out in Paragraph 12.3 for applying patches to vulnerabilities in the Core Information Management System;
- (g) propose interim mitigation measures to vulnerabilities in the Core Information Management System known to be exploitable where a security patch is not immediately available;
- (h) remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in

order to reduce the attack surface of the Core Information Management System);

- (i) inform the Authority when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the Core Information Management System and provide initial indications of possible mitigations;
- (j) produce and maintain Risk Treatment Plans in alignment with a framework to be agreed by the Parties, including supporting Risk Mitigation Evidence Artefacts which provide evidence of risk mitigations; and
- (k) obtain Authority approval for Risk Treatment Plans and Security Case Compliance Statements (including Risk Position Statements and supporting Risk Mitigation Evidence Artefacts), in respect of any of the Services in accordance with the timescales agreed with the Authority.

12.7 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under Paragraph 12.3 and 12.4, the Supplier shall immediately notify the Authority.

12.8 If the Supplier fails to patch vulnerabilities in the Core Information Management System in accordance with Paragraph 12.3 and 12.4, such failure shall constitute a material Default and the Authority may by terminate this Contract with immediate effect by issuing a Termination Notice to the Supplier.

13. Breach of Security

13.1 If either party becomes aware of a Breach of Security, it shall notify the other in accordance with the Incident Management Process.

13.2 The Incident Management Process shall, as a minimum, require the Supplier to do the following upon it becoming aware of a Breach of Security or attempted Breach of Security:

- (a) immediately take all reasonable steps necessary to:
 - (i) minimise the extent of actual or potential harm caused by such Breach of Security;
 - (ii) remedy such Breach of Security to the extent possible;
 - (iii) apply a tested mitigation against any such Breach of Security; and
 - (iv) prevent a further Breach of Security in the future which exploits the same root cause failure;

- (b) as soon as reasonably practicable for critical events, and for other events no later than 48 hours, 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.
- 13.3 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance by the Supplier, its Sub-contractors and/or all or any part of the Core Information Management System or Wider Information Management System with this Contract, then such remedial action shall be completed at no additional cost to the Authority.
- 13.4 If the Supplier fails to comply with its obligations set out in this Paragraph 13, 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 with immediate effect by issuing a Termination Notice to the Supplier.

14. Data Processing, Storage, Management and Destruction

- 14.1 The Supplier's obligations in respect of Processing Personal Data and compliance with the Data Protection Legislation are set out in Clause 21.
- 14.2 In addition to the obligations on the Supplier set out in the Contract in respect of Processing Personal Data and compliance with the Data Protection Legislation, the Supplier shall:
 - (a) ensure that Authority Data is protected and processed in a secure manner. To achieve this objective, the Authority has a preference that Authority Data (other than Personal Data) shall only be processed (including being stored, processed, located, backed up, viewed, modified, copied, or deleted) within the United Kingdom and the European Economic Area. 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 data is processed, stored, managed and destroyed appropriately.
 - (b) agree any change in location of data storage, processing and administration of Authority Data with the Authority (in accordance with Clause 21 (Protection of Personal Data) if the change relates to the Processing of Personal Data).
 - (c) on demand, provide the Authority with all Authority Data in an agreed open format;
 - (d) upon request, be able to state to the Authority the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Authority Data will be subject to at all times.

SCHEDULE 5 (Security Management)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (e) have documented processes to guarantee availability of Authority Data in the event of the Supplier ceasing to trade;
- (f) securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority; and
- (g) securely destroy all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in the Contract and, in the absence of any such requirements, as directed by the Authority.

ANNEX 1: BASELINE SECURITY REQUIREMENTS**1 Security Classification of Information**

1.1 If the provision of the Services requires the Supplier to Process Authority Data which is classified as:

- (a) OFFICIAL-SENSITIVE, the Supplier shall implement such 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; and/or
- (b) SECRET or TOP SECRET, the Supplier shall only do so where it has notified the Authority prior to 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 End User Devices

2.1 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;
- (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;
- (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.

- 2.2 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.

3 Encryption

- 3.1 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.
- 3.2 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 may require.
- 3.3 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.
- 3.4 Where the Authority and Supplier reach agreement, the Supplier must update the Security Management Plan to include:
- 3.4.1 the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and
 - 3.4.2 the protective measure that the Supplier and/or Sub-contractor will put in place in respect of the unencrypted Authority Data.
- 3.5 Where the Authority and Supplier do not reach agreement within 20 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.

4 Personnel Security

- 4.1 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.
- 4.2 "The Authority and the Supplier shall review the roles and responsibilities of Supplier Personnel to ensure they hold the appropriate level of national security vetting clearance. The level required will be determined by the criteria set out within the Cyber and Technical Security Guidance document which can be accessed in Annex C Section 9 of the Statement of Requirements, and the "Minimum User Clearance Requirements Guide" (<https://security-guidance.service.justice.gov.uk/minimum-user-clearance-requirements-guide/#minimum-user-clearance-requirements-guide>)
- 4.3 The Supplier shall not permit Supplier Personnel who fail the security checks required by Paragraphs 4.1 and 4.2 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.
- 4.4 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.
- 4.5 The Supplier shall ensure that Supplier Personnel who no longer require access to the Authority Data (e.g. they cease to be employed by the Supplier or any of its Sub-contractors), have their rights to access the Authority Data revoked within 1 Working Day.
- 4.6 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.
- 4.7 The Supplier shall ensure that the training provided to Supplier Personnel under Paragraph 4.6 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").

5 Identity, Authentication and Access Control

- 5.1 The Supplier shall operate an access control regime to ensure:

- (a) all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and
 - (b) all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.
- 5.2 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 persons access to the Supplier System and Sites so that such persons are allowed access only to those parts of the Sites and the Supplier System they require.
- 5.3 The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such record available to the Authority on request.

6 Data Destruction or Deletion

6.1 The Supplier shall:

- (a) prior to securely sanitising any Authority Data or when requested the Supplier shall provide the Government with all Authority Data in an agreed open format;
- (b) have documented processes to ensure the availability of Authority Data in the event of the Supplier ceasing to trade;
- (c) 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;
- (d) 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
- (e) implement processes which address the CPNI and NCSC guidance on secure sanitisation.

7 Audit and Protective Monitoring Reporting

- 7.1 The Supplier shall collect 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 Supplier audit records should (as a minimum) 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.
- 7.2 In addition to any requirement in Clause 37.3, the Supplier shall

- (a) Implement audit and monitoring of the Core Information Management System sufficient to comply with any applicable Relevant Requirements and to prevent or detect any Prohibited Act;
 - (b) Keep sufficient records to demonstrate compliance with the requirements of Paragraph 6 to the Authority; and
 - (c) Make those records and any documents describing the audit and monitoring undertaken to the Authority on request.
- 7.3 The Supplier and the Authority shall work together to establish any additional audit and monitoring requirements for the Core Information Management System.
- 7.4 The retention periods for audit records and event logs must be agreed with the Authority and documented in the Security Management Plan.
- 7.5 The Supplier shall arrange independent reviews and assessments by a United Kingdom Accreditation Service (UKAS) accredited certification body to ensure certifications are maintained in line with the National Cyber Security Centre Cyber Assessment Framework.
- 7.6 The Supplier shall provide the Authority with reporting information with regards to risk management using the National Cyber Security Centre Cyber Assessment Framework and upon request by the Authority, provide information relating to risk, risk likelihood, risk impact and mitigating actions:
- 7.6.1 The Supplier shall provide status reports to the Authority on a monthly basis in advance of the relevant Board, as agreed at the relevant Boards from time to time; and
 - 7.6.2 The Supplier shall issue status reports for new vulnerabilities, mitigations, or incidents, and shall also detail the action taken to mitigate and/or remediate the risk, including in accordance with the Security Management Plan.

8 Location of Authority Data

- 8.1 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 ensure that Authority Data is protected and processed in a secure manner. To achieve this objective, the Authority has a preference that Authority Data (other than Personal Data) shall only be processed (including being stored, processed, located, backed up, viewed, modified, copied, or deleted) within the United Kingdom and the European Economic Area. 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 data. In addition, appropriate measures must be put in place to prevent unauthorized access, use, or disclosure of the data.

- 8.2 The Supplier shall agree any change in location of data storage, processing and administration of Authority Data with the Authority (in accordance with Clause 21 (Protection of Personal Data) if the change relates to the Processing of Personal Data

9 Vulnerabilities and Corrective Action

- 9.1 The Authority and the Supplier acknowledge that vulnerabilities in the Core Information Management System may be discovered which unless mitigated will present an unacceptable risk to the Authority Data.
- 9.2 The severity of vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'High', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the Security Management Plan and using the appropriate vulnerability scoring systems including:
- (a) 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
 - (b) Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.
- 9.3 Subject to Paragraph 9.4, the Supplier shall procure the application of security patches to vulnerabilities in the Core Information Management System within:
- (a) seven (7) days after the public release of patches for those vulnerabilities categorised as 'Critical';
 - (b) thirty (30) days after the public release of patches for those vulnerabilities categorised as 'High' or 'Important'; and
 - (c) sixty (60) days after the public release of patches for those vulnerabilities categorised as 'Medium' or 'Moderate' or 'Low'.
- 9.4 The timescales for applying patches set out in Paragraph 9.3 shall be extended where:
- (a) the Supplier can demonstrate that a vulnerability in the Core Information Management System is not exploitable (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 9.3 if the vulnerability becomes exploitable within the context of the Services;
 - (b) 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,

provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or

- (c) 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.

9.5 The Security Management Plan shall include provisions for major version upgrades of all LAN Software to be kept up to date such that all LAN Software is always in mainstream support throughout the Term unless otherwise agreed by the Authority in writing. All LAN Software should be no more than N-1 versions behind the latest software release.

10 Secure Architecture

10.1 The Supplier shall design the Core Information Management System in accordance with:

- (a) 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>;
- (b) 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
- (c) 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:
 - (i) "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;
 - (ii) "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;
 - (iii) "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;
 - (iv) "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;

- (v) "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;
- (vi) "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;
- (vii) "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;
- (viii) "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;
- (ix) "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;
- (x) "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;
- (xi) "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;
- (xii) "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;
- (xiii) "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
- (xiv) "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 Core Information Management System.

ANNEX 2: SECURITY REQUIREMENTS FOR SUB-CONTRACTORS

1 Application of Annex

1.1 This Annex 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;
- (b) keep sufficient records to demonstrate that compliance to the Authority; and
- (c) ensure that the Detailed 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 When designing and configuring the Operating Environment (to the extent that the Operating Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a NCSC Certified Cyber Professional certification for all bespoke or complex components of the Operating Environment (to the extent that the Operating Environment is within the control of the Supplier).

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>,
- (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-security?curPage=/collection/cloud-security/implementing-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's obligations in respect of Processing Personal Data and compliance with the Data Protection Legislation are set out in Clause 21. The Supplier shall ensure that Authority Data is protected and processed in a

secure manner. To achieve this objective, the Authority has a preference that Authority Data (other than Personal Data) shall only be processed (including being stored, processed, located, backed up, viewed, modified, copied, or deleted) within the United Kingdom and the European Economic Area. 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 data. In addition, appropriate measures must be put in place to prevent unauthorized access, use, or disclosure of the data. The Supplier shall agree any change in location of data storage, processing and administration of Authority Data with the Authority (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:
- 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;
 - 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;
 - 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.
- 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 Contract.

6 Encryption

- 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 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 may require.
- 6.3 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.
- 6.4 Where the Authority and Supplier reach agreement, the Supplier must update the 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.
- 6.5 Where the Authority and Supplier 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.
- 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 software purport to grant the licensor rights to Progress the Authority Data greater than those rights strictly necessary for the use of the software.

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 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 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

<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	C1: Internet-facing firewalls	Very low

ANNEX 3: (Security Management Plan Template)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
			internet via the web portal.	C2: Internet-facing IP whitelist 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	Low

ANNEX 3: (Security Management Plan Template)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
				sent to users' home addresses when 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/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>

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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 6

INSURANCE REQUIREMENTS

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
 - (c) hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance

SCHEDULE 6 (Insurance Requirements)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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.

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 £100,000 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 £10,000,000 in respect of any one occurrence, the number of occurrences being unlimited in any annual policy period, but £ 10,000,000 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.**

ANNEX 1: (Required Insurances)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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.

3 Limit of indemnity

- 3.1 Not less than five million pounds (£5,000,000) in respect of any one claim and in the aggregate per annum.

ANNEX 1: (Required Insurances)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 7
AUTHORITY RESPONSIBILITIES

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 and the Paragraphs of the Schedules (except Schedule 2 (*Services Description*) and Schedule 8 (*Supplier Solution*));
- (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).

SCHEDULE 7 (Authority Responsibilities)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**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:

ID	Relevant Document	Authority Responsibility
AO-001	Schedule 14 (Testing Procedures)	The Authority shall support the Supplier in the planning, design, implementation, execution and reporting of maintenance release Testing in accordance with Schedule 14 (Testing Procedures) within a reasonable timescale of receiving the Supplier's request.
AO-002	Schedule 2 (Services Description) – Annex B – LAN Service Management Requirements	The Authority shall provide and maintain the Authority's ITSM Toolset and the ITSM data within the Authority's ITSM Toolset as is reasonably required to allow the Supplier to establish connection for the exchange of near real-time data and/or to access and utilise it.
AO-003		NOT USED
AO-004	Schedule 2 (Services Description) – Annex A – LAN Technical Requirements	The Authority shall be responsible for the provision of WAN transport, WAN overlay, and WAN security necessary to connect the LAN Services to the WAN and Internet.
AO-005	Schedule 2 (Services Description) – Annex A – LAN Technical Requirements	Where the Authority agrees to hold spare parts on Authority Sites, these shall be stored in a secure manner.
AO-006	Schedule 2 (Services Description) – Annex A – LAN Technical Requirements	The Authority shall provide, maintain and support the Network Access Control (NAC) services required for the LAN Services with the exception of the NAC services to be provided by the Supplier in accordance with Section 2.4.2 of Annex A (LAN Technical Requirements) to Schedule 2 (Services Description).
AO-007	Schedule 2 (Services	The Authority shall be responsible for the:

SCHEDULE 7 (Authority Responsibilities)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

ID	Relevant Document	Authority Responsibility
	Description) – Annex A – LAN Technical Requirements	• Provision of power and cooling services; • Provision of security and access control services; • Provision of uninterrupted power supply services; • Management of the rack space allocation and availability; within Local ICT Rooms through the relevant Other Suppliers.
AO-008	Schedule 3 (Performance Levels)	The Authority shall provide a single point of contact for End Users (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: • liaise with appropriately trained and skilled expert resource from the Supplier as required to handle the End User’s query; • handle End Users 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; • manage progress of Incidents through the Incident lifecycle utilising the Supplier updates recorded in the ITSM Toolset, and update the End User on progress; • update End Users in a timely and accurate manner with any updates recorded in the ITSM Toolset.

SCHEDULE 8 (Supplier Solution)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 8
SUPPLIER SOLUTION



Supplier Solution

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]		
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED] [REDACTED] [REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED]	[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

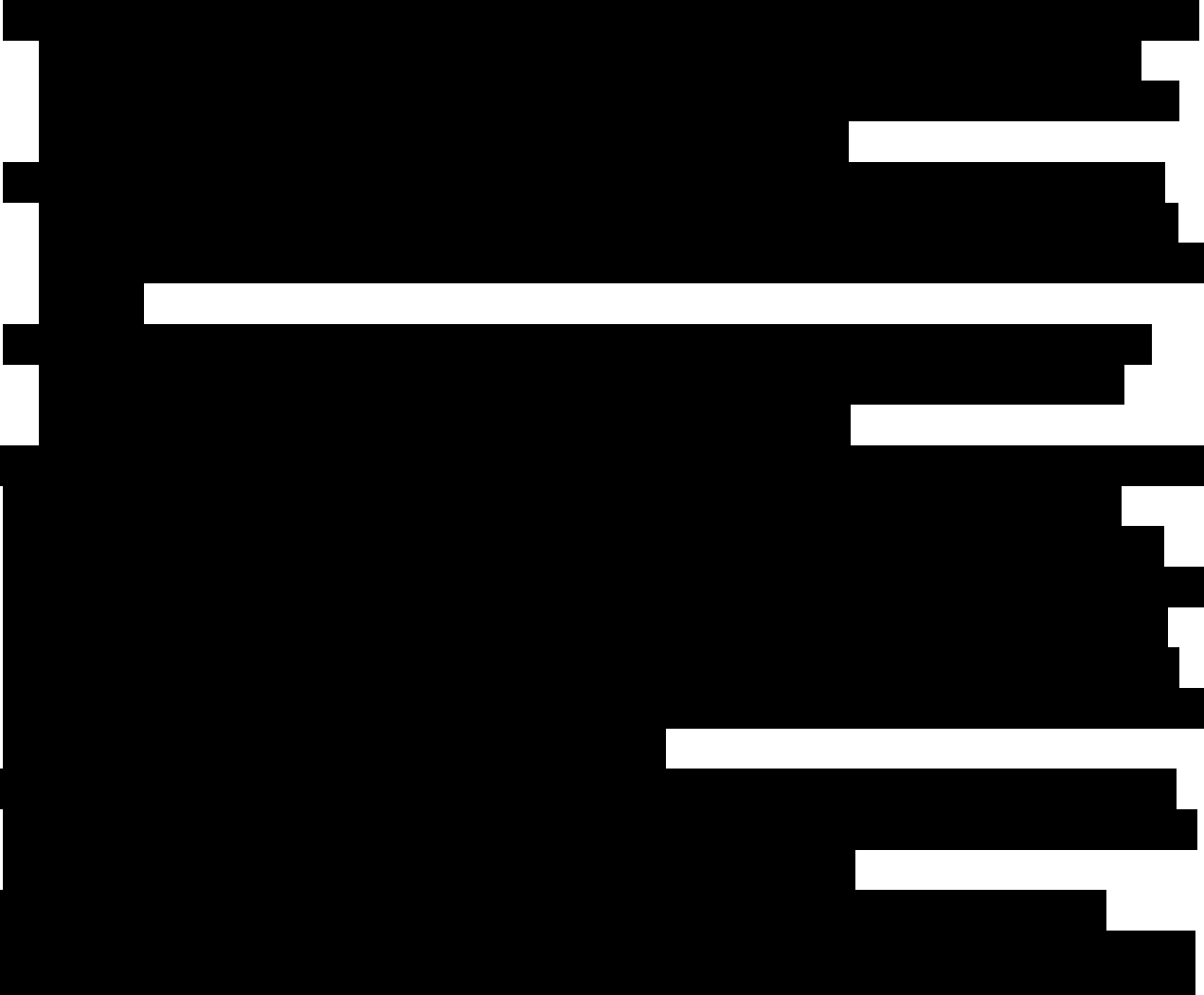
[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[illegible]

A large black rectangular redaction box covers the majority of the page, obscuring all text and graphics. Only a few horizontal white lines are visible, suggesting the presence of a table or multiple lines of text that have been completely hidden.

[illegible]

[REDACTED]

Case	Case	Case	Case
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

	2019	2020	2021
1. Overall	100%	100%	100%
2. By Region			
2.1. North	100%	100%	100%
2.2. South	100%	100%	100%
2.3. East	100%	100%	100%
2.4. West	100%	100%	100%
3. By Sector			
3.1. Health	100%	100%	100%
3.2. Economy	100%	100%	100%
3.3. Education	100%	100%	100%
3.4. Environment	100%	100%	100%
3.5. Social	100%	100%	100%
4. By Country			
4.1. USA	100%	100%	100%
4.2. UK	100%	100%	100%
4.3. Germany	100%	100%	100%
4.4. France	100%	100%	100%
4.5. Italy	100%	100%	100%
4.6. Spain	100%	100%	100%
4.7. China	100%	100%	100%
4.8. India	100%	100%	100%
4.9. Japan	100%	100%	100%
4.10. South Korea	100%	100%	100%
4.11. Canada	100%	100%	100%
4.12. Australia	100%	100%	100%
4.13. Brazil	100%	100%	100%
4.14. India	100%	100%	100%
4.15. China	100%	100%	100%
4.16. USA	100%	100%	100%
4.17. UK	100%	100%	100%
4.18. Germany	100%	100%	100%
4.19. France	100%	100%	100%
4.20. Italy	100%	100%	100%
4.21. Spain	100%	100%	100%
4.22. China	100%	100%	100%
4.23. India	100%	100%	100%
4.24. Japan	100%	100%	100%
4.25. South Korea	100%	100%	100%
4.26. Canada	100%	100%	100%
4.27. Australia	100%	100%	100%
4.28. Brazil	100%	100%	100%
4.29. India	100%	100%	100%
4.30. China	100%	100%	100%
4.31. USA	100%	100%	100%
4.32. UK	100%	100%	100%
4.33. Germany	100%	100%	100%
4.34. France	100%	100%	100%
4.35. Italy	100%	100%	100%
4.36. Spain	100%	100%	100%
4.37. China	100%	100%	100%
4.38. India	100%	100%	100%
4.39. Japan	100%	100%	100%
4.40. South Korea	100%	100%	100%
4.41. Canada	100%	100%	100%
4.42. Australia	100%	100%	100%
4.43. Brazil	100%	100%	100%
4.44. India	100%	100%	100%
4.45. China	100%	100%	100%
4.46. USA	100%	100%	100%
4.47. UK	100%	100%	100%
4.48. Germany	100%	100%	100%
4.49. France	100%	100%	100%
4.50. Italy	100%	100%	100%
4.51. Spain	100%	100%	100%
4.52. China	100%	100%	100%
4.53. India	100%	100%	100%
4.54. Japan	100%	100%	100%
4.55. South Korea	100%	100%	100%
4.56. Canada	100%	100%	100%
4.57. Australia	100%	100%	100%
4.58. Brazil	100%	100%	100%
4.59. India	100%	100%	100%
4.60. China	100%	100%	100%
4.61. USA	100%	100%	100%
4.62. UK	100%	100%	100%
4.63. Germany	100%	100%	100%
4.64. France	100%	100%	100%
4.65. Italy	100%	100%	100%
4.66. Spain	100%	100%	100%
4.67. China	100%	100%	100%
4.68. India	100%	100%	100%

	</		

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]



[illegible]

Scaling Capacity for Future Authority Initiatives

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Asset Tracking and Software Maintenance and Patching

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Managing Escalations

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

Category	Sub-category	Item	Value	Unit	Description
A	1	1	100	kg	Item 1
		2	200	kg	Item 2
		3	300	kg	Item 3
		4	400	kg	Item 4
		5	500	kg	Item 5
B	2	1	100	kg	Item 1
		2	200	kg	Item 2
		3	300	kg	Item 3
		4	400	kg	Item 4
		5	500	kg	Item 5
C	3	1	100	kg	Item 1
		2	200	kg	Item 2
		3	300	kg	Item 3
		4	400	kg	Item 4
		5	500	kg	Item 5
D	4	1	100	kg	Item 1
		2	200	kg	Item 2
		3	300	kg	Item 3
		4	400	kg	Item 4
		5	500	kg	Item 5
E	5	1	100	kg	Item 1
		2	200	kg	Item 2
		3	300	kg	Item 3
		4	400	kg	Item 4
		5	500	kg	Item 5

1	2	3	4	5	6
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	101	102
103	104	105	106	107	108
109	110	111	112	113	114
115	116	117	118	119	120
121	122	123	124	125	126
127	128	129	130	131	132
133	134	135	136	137	138
139	140	141	142	143	144
145	146	147	148	149	150
151	152	153	154	155	156
157	158	159	160	161	162
163	164	165	166	167	168
169	170	171	172	173	174
175	176	177	178	179	180
181	182	183	184	185	186
187	188	189	190	191	192
193	194	195	196	197	198
199	200	201	202	203	204
205	206	207	208	209	210
211	212	213	214	215	216
217	218	219	220	221	222
223	224	225	226	227	228
229	230	231	232	233	234
235	236	237	238	239	240
241	242	243	244	245	246
247	248	249	250	251	252
253	254	255	256	257	258
259	260	261	262	263	264
265	266	267	268	269	270
271	272	273	274	275	276
277	278	279	280	281	282
283	284	285	286	287	288
289	290	291	292	293	294
295	296	297	298	299	300
301	302	303	304	305	306
307	308	309	310	311	312
313	314	315	316	317	318
319	320	321	322	323	324
325	326	327	328	329	330
331	332	333	334	335	336
337	338	339	340	341	342
343	344	345	346	347	348
349	350	351	352	353	354
355	356	357	358	359	360
361	362	363	364	365	366
367	368	369	370	371	372
373	374	375	376	377	378
379	380	381	382	383	384
385	386	387	388	389	390
391	392	393	394	395	396
397	398	399	400	401	402
403	404	405	406	407	408
409	410	411	412	413	414
415	416	417	418	419	420
421	422	423	424	425	426
427	428	429	430	431	432
433	434	435	436	437	438
439	440	441	442	443	444
445	446	447	448	449	450
451	452	453	454	455	456
457	458	459	460	461	462
463	464	465	466	467	468
469	470	471	472	473	474
475	476	477	478	479	480
481	482	483	484	485	486
487	488	489	490	491	492
493	494	495	496	497	498
499	500	501	502	503	504
505	506	507	508	509	510
511	512	513	514	515	516
517	518	519	520	521	522
523	524	525	526	527	528
529	530	531	532	533	534
535	536	537	538	539	540
541	542	543	544	545	546
547	548	549	550	551	552
553	554	555	556	557	558
559	560	561	562	563	564
565	566	567	568	569	570
571	572	573	574	575	576
577	578	579	580	581	582
583	584	585	586	587	588
589	590	591	592	593	594
595	596	597	598	599	600
601	602	603	604	605	606
607	608	609	610	611	612
613	614	615	616	617	618
619	620	621	622	623	624
625	626	627	628	629	630
631	632	633	634	635	636
637	638	639	640	641	642
643	644	645	646	647	648
649	650	651	652	653	654
655	656	657	658	659	660
661	662	663	664	665	666
667	668	669	670	671	672
673	674	675	676	677	678
679	680	681	682	683	684
685	686	687	688	689	690
691	692	693	694	695	696
697	698	699	700	701	702
703	704	705	706	707	708
709	710	711	712	713	714
715	716	717	718	719	720
721	722	723	724	725	726
727	728	729	730	731	732
733	734	735	736	737	738
739	740	741	742	743	744
745	746	747	748	749	750
751	752	753	754	755	756
757	758	759	760	761	762
763	764	765	766	767	768
769	770	771	772	773	774
775	776	777	778	779	780
781	782	783	784	785	786
787	788	789	790	791	792
793	794	795	796	797	798
799	800	801	802	803	804
805	806	807	808	809	810
811	812	813	814	815	816
817	818	819	820	821	822
823	824	825	826	827	828
829	830	831	832	833	834
835	836	837	838	839	840
841	842	843	844	845	846
847	848	849	850	851	852
853	854	855	856	857	858
859	860	861	862	863	864
865	866	867	868	869	870
871	872	873	874	875	876
877	878	879	880	881	882
883	884	885	886	887	888
889	890	891	892	893	894
895	896	897	898	899	900
901	902	903	904	905	906
907	908	909	910	911	912
913	914	915	916	917	918
919	920	921	922	923	924
925	926	927	928	929	930
931	932	933	934	935	936
937	938	939	940	941	942
943	944	945	946	947	948
949	950	951	952	953	954
955	956	957	958	959	960
961	962	963	964	965	966
967	968	969	970	971	972
973	974	975	976	977	978
979	980	981	982	983	984
985	986	987	988	989	990
991	992	993	994	995	996
997	998	999	1000	1001	1002
1003	1004	1005	1006	1007	1008
1009	1010	1011	1012	1013	1014
1015	1016	1017	1018	1019	1020
1021	1022	1023	1024	1025	1026
1027	1028	1029	1030	1031	1032
1033	1034	1035	1036	1037	1038
1039	1040	1041	1042	1043	1044
1045	1046	1047	1048	1049	1050
1051	1052	1053	1054	1055	1056
1057	1058	1059	1060	1061	1062
1063	1064	1065	1066	1067	1068
1069	1070	1071	1072	1073	1074
1075	1076	1077	1078	1079	1080
1081	1082	1083	1084	1085	1086
1087	1088	1089	1090	1091	1092
1093	1094	1095	1096	1097	1098
1099	1100	1101	1102	1103	1104
1105	1106	1107	1108	1109	1110
1111	1112	1113	1114	1115	1116
1117	1118	1119	1120	1121	1122
1123	1124	1125	1126	1127	1128
1129	1130	1131	1132	1133	1134
1135	1136	1137	1138	1139	1140
1141	1142	1143	1144	1145	1146
1147	1148	1149	1150	1151	1152
1153	1154	1155	1156	1157	1158
1159	1160	1161	1162	1163	1164
1165	1166	1167	1168	1169	1170
1171	1172	1173	1174	1175	1176
1177	1178	1179	1180	1181	1182
1183	1184	1185	1186	1187	1188
1189	1190	1191	1192	1193	1194
1195	1196	1197	1198	1199	1200
1201	1202	1203	1204	1205	1206
1207	1208	1209	1210	1211	1212
1213	1214	1215	1216	1217	1218
1219	1220	1221	1222	1223	1224
1225	1226	1227	1228	1229	1230
1231	1232	1233	1234	1235	1236
1237	1238	1239	1240	1241	1242
1243	1244	1245	1246	1247	1248
1249	1250	1251	1252	1253	1254
1255	1256	1257	1258	1259	1260
1261	1262	1263	1264	1265	1266
1267	1268	1269	1270	1271	1272
1273	1274	1275	1276	1277	1278
1279	1280	1281	1282	1283	1284
1285	1286	1287	1288	1289	1290
1291	1292	1293	1294	1295	1296
1297	1298	1299	1300	1301	1302
1303	1304	1305	1306	1307	1308
1309	1310	1311	1312	1313	1314
1315	1316	1317	1318	1319	1320
1321	1322	1323	1324	1325	1326
1327	1328	1329	1330	1331	1332
1333	1334	1335	1336	1337	1338
1339	1340	1341	1342	1343	1344
1345	1346	1347	1348	1349	1350
1351	1352	1353	1354	1355	1356
1357	1358	1359	1360	1361	1362
1363	1364	1365	1366	1367	1368
1369	1370	1371	1372	1373	1374
1375	1376	1377	1378	1379	1380
1381	1382	1383	1384	1385	1386
1387	1388	1389	1390	1391	13

Schedule 8 – Supplier Solution

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[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

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[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

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[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

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
					[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
					[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
					[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
					[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
					[REDACTED]

[illegible]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[Redacted text block]

[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]

[Redacted text block]



Evaluation and Classification of Risks

[Redacted]

[Redacted]

Managing and Treating Risks

[Redacted]

[Redacted]		[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Vulnerability Management

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED] and
- Support as standard for multicast and anycast traffic. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Providing Consistency in Design Standards and Controls

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[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

[REDACTED]

[REDACTED]

Scalability

[REDACTED]

[REDACTED]

Performance

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1. **Identify the main components of the system.**

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Phased Migration Approach – Access Switch Segmentation and Zero Trust

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Maintaining, Managing, and Implementing changes to the LAN Services Cabling

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

• [REDACTED], empty cable

[REDACTED] boxes, rubbish etc. must be removed from site on a daily basis. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

Schedule 8 – Supplier Solution

[illegible]

Page 186 of 1059

Schedule 8 – Supplier Solution

[illegible]

Schedule 8 – Supplier Solution

Schedule 8 – Supplier Solution

[illegible]

Schedule 8 – Supplier Solution

[illegible]

[illegible]

[illegible]

[illegible]

Schedule 8 – Supplier Solution

[illegible]

Schedule 8 – Supplier Solution

[REDACTED]	
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Page 198 of 1059

Schedule 8 – Supplier Solution

[illegible]

Schedule 8 – Supplier Solution

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]



		[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]	
		[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
[REDACTED]		[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]
		[REDACTED]	[REDACTED]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]



[Redacted text block]

Schedule 8 – Supplier Solution



Schedule 8 – Supplier Solution

Annex 3 – The Supplier’s ALT Response

Submitted FRT Cost Breakdown

Schedule 8 – Supplier Solution

[REDACTED]

[REDACTED]

Schedule 8 – Supplier Solution

[REDACTED]

The Supplier’s TUPE Costs Information Worksheet

SCHEDULE 9

COMMERCIALLY SENSITIVE INFORMATION

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		[REDACTED]	[REDACTED]
2		[REDACTED]	[REDACTED]
3		[REDACTED]	[REDACTED]

SCHEDULE 10

NOTIFIED KEY SUB-CONTRACTORS

SCHEDULE 10 (Notified Key Sub-Contractors)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**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]	[REDACTED] BE .257.869	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

SCHEDULE 10 (Notified Key Sub-Contractors)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 11 (Third Party Contracts)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 11
THIRD PARTY CONTRACTS

SCHEDULE 11 (Third Party Contracts)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**Schedule 11 (*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]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

SCHEDULE 12

SOFTWARE

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.

2 SUPPLIER SOFTWARE

The Supplier Software includes the following items:

The Supplier confirms that they are not providing any Supplier Software to the Authority as part of their solution.

Software	Supplier (if an Affiliate of the Supplier)	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/Expiry
■	■	■	■	■	■	■	■

3 THIRD PARTY SOFTWARE

As part of the Contract the Supplier shall provide two components specific for the management for the Authority’s network as software as a service (SaaS).

[REDACTED]

[REDACTED]

Each LAN device within the Authority’s network will have a licensed operating software installed. The Ownership of this Software remains with the Authority. The verification and quantities of this will need defining at the network verification stage of the contract delivery.

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]

**ANNEX 1: FORM OF LETTER RE SUB-LICENSING OF SUPPLIER COTS
SOFTWARE AND SUPPLIER COTS BACKGROUND IPRs**

[Supplier letterhead]

**[insert Authority
name and address]**

[Date]

Dear Sirs

**LICENCES FOR SUPPLIER COTS SOFTWARE AND SUPPLIER 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 2.4(b) **[use this if Options 1 or 2 in Schedule 32
(Intellectual Property Rights) are chosen]** [2.5(b) **[use this if Options 3 or 4 in
Schedule 32 (Intellectual Property Rights) are used]**] of Schedule 32 (*Intellectual
Property Rights* of the Contract we confirm that:

- 1 the Authority is licensed by the Supplier to use the Supplier COTS Software
and Supplier 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 may sub-license, assign and novate the Supplier COTS Software
and Supplier COTS Background IPRs as referred to in Paragraph [2.4(b) **[use
this if Options 1 or 2 in Schedule 32 (Intellectual Property Rights) are chosen]**
[2.5(b) **[use this if Options 3 or 4 in Schedule 32 (Intellectual Property Rights
are used)]**] of Schedule 32 (*Intellectual Property Rights* of the Contract.

Yours faithfully,

Signed:

On behalf of **[name of the Supplier]**

ANNEX 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) **[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 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:
 - (e) was in the possession of the Sub-licensee without obligation of confidentiality prior to its disclosure by the Authority;
 - (f) 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
 - (g) 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.

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 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 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:

ANNEX 2: (Form of Confidentiality Undertaking)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

[Name of Organisation]

[Address]

Attention: []

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:

SCHEDULE 13 (Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 13

IMPLEMENTATION PLAN

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 12 months,

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

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

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 and any Authority Responsibilities set out in the Outline Implementation Plan will no longer apply and will be replaced by those set out in the approved 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 Service Management 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 Exit and Transition 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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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.

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 Product Description for the relevant Documentary Deliverable., which sets out the Quality Criteria that the Documentary Deliverable must meet in order to be Approved.

Development of Product Descriptions for Documentary Deliverables

- 1.5 Other than where the Product Description is already in existence under this Contract as set out at Annex 3 to this Schedule 13, 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 Product Description materially in the format specified at Annex 2 to this Schedule 13 and/or in accordance with any applicable, more specific template Product Description under this Contract and shall make the draft Product Description available to the Authority for review.
- 1.6 The Supplier shall ensure that the Product 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.
- 1.7 The Authority shall review the draft Product 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 Product 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 Product Description and shall notify the Supplier of the outcome of the review, within ten (10) Working

Days of the Authority receiving the draft Product Description, or within such other period as may be agreed between the Parties.

- 1.9 Where the draft Product Description meets the criteria set out in Paragraph 1.7 of this Part B, the Authority shall notify its agreement of the Product Description in writing to the Supplier.
- 1.10 Where the draft Product 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 Product 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 Product 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;
 - 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 Product 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:
 - 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 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

SCHEDULE 13 (Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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.

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**ANNEX 1: OUTLINE IMPLEMENTATION PLAN**

Milestone	Deliverables (bulleted list showing all Deliverables (and associated tasks/approvals/unconditional Test Certificates) required for each Milestone)	Duration (Working Days)	Milestone Date	Authority Responsibilities (if applicable)	Link to ATP/CPP Key Milestone, subject to Delay Payments (Y/N)
M1 - Draft Detailed Implementation Plan Documentary Deliverable	• The Supplier has provided the Detailed Implementation Plan (Schedule 13 - Implementation Plan), including the initial baseline site lifecycle and migration approach outlining how M10 - Fixed LAN and Wireless Services Transition will be delivered. The plan will be capable of being approved by the Authority in accordance with Paragraph 3, Part A of this Schedule. • The Supplier has provided a baseline version of the Draft Detailed Implementation Plan in a format acceptable to the Authority (e.g., MS Project Plan). The Draft Detailed Implementation Plan will be capable of Authority approval in accordance with Part B of this Schedule.	20 Working Days	Effective Date + 40 Working Days	Not applicable	Not applicable

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	• The Supplier has provided a Test Strategy, (Schedule 14 - Testing Procedures) in accordance with Paragraph 4 of Schedule 14. • The Supplier has provided a Requirements traceability matrix (RTM) in the format provided by the Authority). • Transition Framework deliverables: the Parties have reviewed the "Transition Framework" and agreed the Documentary Deliverables relevant to the Implementation Services which correspond to the artefacts listed for each gate of the Transition Framework. • The Supplier has provided Product Descriptions for Documentary Deliverables for the next dependent Milestones.				
M2 – Contract Setup Complete Documentary Deliverable	• The Supplier has provided an in-flight project and interim service requests report which is capable of Authority approval. (LAN Transition Requirements (Schedule 2 Annex C). • The Supplier has provided proposals for the agreed in-	40 Working Days	Effective Date + 40 Working Days	• Ensure that the information released to the Supplier is in a format that is capable of Supplier review. • Provide baseline list of Authority	Not applicable

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	flight projects and interim service requests which are capable of the Authority approval. The Supplier will provide an invoice template and charging and invoicing processes (Schedule 15 Charges and Invoicing) which are capable of Authority approval in accordance Part B of this Schedule. • The Supplier has provided a Transition governance approach (Schedule 21 Governance) which is capable of Authority approval in accordance with Part B of this Schedule. • The Supplier has provided a baselined Asset and Configuration Items list which is capable of Authority approval. The Asset and Configuration Items list will include the Preceding Services, Service Asset and Configuration Items including Transferring Assets if applicable. The deliverable will baseline the assets that the Supplier will support (LAN Service Management Requirements Schedule 2 Annex B).			Assets and Configurations Items. • Release an in-flight project and interim service request list for Supplier assessment and review. • Provide the Supplier with access to the ITSM Toolset (including the CMDB) in accordance with the Authority Responsibility AO-002 Schedule 7 (Authority Responsibilities).	

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	• The Supplier has evidenced the upload of the baselined Authority Assets and Configuration Items that it will support into the CMDB (LAN Transition Requirements, Paragraph 7.1.2.14. • The Supplier has provided Test Plans (Schedule 14 – Testing Procedures) which are capable of Authority approval in accordance with Paragraph 5 (Test Plans) of Schedule 14 (Testing Procedures). • The Supplier has provided the Security Management Plan (Schedule 5 Security Management) which is capable of Authority approval in accordance with Paragraph 6 of Schedule 5 (Security Management). • The Supplier has provided the Quality Plan (Core Terms – Implementation) which is capable of Authority approval in accordance with Clause 6 Core Terms – Implementation. • The Supplier has provided the communications plan (LAN Transition Requirements Schedule 2 Annex C) which is capable of Authority approval				

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	in accordance with Part B of this Schedule. • The Supplier has provided a Service Continuity Management Plan (Schedule 26 Service Continuity Plan and Corporate Resolution Planning) which is capable of Authority approval in accordance with Paragraph 2 of Schedule 26 (Service Continuity Plan and Corporate Resolution Planning). • The Supplier has provided a Products and Services Catalogue (Schedule 15 Charges and Invoicing) which is capable of Authority approval in accordance with Paragraph 3.4 of Part A of Schedule 15 (Charges and Invoicing). • The Supplier has provided a Provisional Supplier Personnel List (Schedule 28 – Staff Transfer) which is capable of Authority approval in accordance with Part E (Employment Exit Provisions) of Schedule 28. • The Supplier has provided the Sustainability Reports relevant to Waste in accordance with Annex 1 Table C Schedule 4 (Standards).				

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	• The Supplier shall have appointed a Transition Lead. • The Supplier shall have appointed a HR Lead. • The Supplier has achieved “Gate Approval” of Gate 1 (‘Initiation and mobilisation’) as described in the “Transition Framework” Standard. • The Supplier has provided Product Descriptions for Documentary Deliverables for the next dependent Milestones.				
M3 – High Level Design Documentary Deliverable	• The Supplier has provided a High-Level Design for the Monitoring and Management of the LAN as documented in Annex A Technical Requirements which is capable of approval in accordance with Part B of this Schedule. • The Supplier has provided the Authority Site migration approach including the standard set of Site on boarding cycles which is capable of Authority approval in accordance with Part B of this Schedule. • The Supplier has reviewed and agreed with the Authority the business priorities and	20 Working Days	Effective Date + 40 Working Days	Not applicable	Not applicable

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	constraints that have been identified and impacted for Authority Sites. • The Supplier has provided Product Descriptions for Documentary Deliverables for the next dependent Milestones.				
M4 - Service and Solution Design Complete Documentary Deliverable	• The Supplier has provided a Hard LAN Services support Service Design Package (LAN Service Management Requirements (Schedule 2 Annex B) which is capable of Authority approval in accordance with Part B of this Schedule. • The Supplier has provided a Soft LAN Services support Service Design Package (LAN Service Management Requirements (Schedule 2 Annex B) which is capable of Authority approval in accordance with Part B of this Schedule. • The Supplier has provided documentation, which is capable of approval in accordance with Part B of this Schedule, that describes the Deployed Architecture of the Services (LAN Transition	30 Working Days	Effective Date + 50 Working Days	• Assure interoperability of the Supplier's operating model with wider services in the Authority's service management environment; provide input into the Service Design Packages developed by the Supplier and detail how the Authority's service management environment operates. • The Authority to support the Supplier's DMMP integration workshops.	Not applicable

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	Requirements Schedule 2 Annex C). • The Supplier has evidenced that the Device Management and Monitoring Platform (DMMP) integration workshops completed. • The Supplier has provided a training approach (LAN Service Management Requirements Schedule 2 Annex B) which is capable of Authority approval in accordance with Part B of this Schedule. • The Supplier has agreed with the Authority the aim and scope of the first IT Health Check of the Information Management System. • The Supplier has provided a Solution Design which is capable of Authority approval in accordance with Part B of this Schedule and details the DMMP integration. • The Supplier has met the applicable Quality Criteria for the Service Monitoring and Management of the LAN estate (LAN Detailed Technical Requirements (Schedule 2 Annex A) for the Service				

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	Monitoring and Management of the LAN estate schedule. • The Supplier has provided Product Descriptions for Documentary Deliverables for the next dependent Milestones. • “Gate Approval” of Gate 2 (‘Detailed Design Complete’) as described in the “Transition Framework” Standard.				
M5 - Hard LAN Services Acceptance Sign Off Non -Documentary Deliverable First Operational Service Commencement Date	• The Supplier has provided confirmation that the Hard LAN Services Resource on boarding is complete. • The Supplier has provided confirmation that Supplier Hard LAN Services support resources have been granted security clearance. • The Supplier has provided confirmation that the Supplier has physical access to Authority Sites. • The Supplier has provided the Hard LAN Services service management processes and procedures which are capable of integration with the Authority service management processes and procedures. The service management processes and procedures will	50 Working Days	Effective Date + 60 Working Days	• Support access requests to Authority Sites in accordance with Schedule 7 (Authority Responsibilities) • Schedule and chair Service Readiness Review meetings	ATP Milestone. The Supplier must have Achieved this Milestone 5 before it can commence provision of the relevant Operational Services Key Milestone (Y)

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	be capable of Authority approval in accordance with requirement 6.7.2.8 LAN Service Management Requirements Schedule 2 (Annex B). • The Supplier has provided Authority approved ITSCM awareness and training for all their ITSCM related personnel (LAN Transition Requirements Schedule 2 Annex C). • The Supplier has evidenced that the Hard LAN Services training is complete. • Post Go Live Report: Approval Success: Quality Criteria to include: "as specified in requirements in Paragraph 7.1.2.5 of the Transition Requirements". • The Supplier has evidenced that the Hard LAN Services service management and operational processes testing complete in accordance with Schedule 14 (Testing Procedures). • The Supplier has provided a Test Plan which is capable of Authority approval in accordance with Paragraph 5				

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	of Schedule 14 (Testing Procedures). • The Supplier has provided a Test Specification in accordance with Paragraph 7 of Schedule 14 (Testing Procedures). • The Supplier has been issued with Test Certificates by the Authority for the testing of the Hard LAN Services operational processes having satisfied the Test Success Criteria in accordance with Schedule 14 (Testing Procedures). • The Supplier has provided a draft and final Test Report in accordance with Paragraph 8 of Schedule 14 (Testing Procedures). • The Supplier has achieved Milestone Achievement Certificate sign off for Milestones 1, 2, 3 and 4. • The Supplier has provided Product Descriptions for the next Milestone. • "Gate Approval" of Gate 3 ('Build and Test') and Gate 4 ('Cutover to Service Commencement') as described				

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	in the "Transition Framework" Standard. On completion of this Milestone the Supplier has Achieved The First Operational Service Commencement Date for the Hard LAN Services.				
M6 – Soft LAN Services and Tooling Testing Sign Off Non -Documentary Deliverable	- The Supplier has provided a Test Plan which is capable of Authority approval in accordance with Paragraph 5 of Schedule 14 (Testing Procedures). - The Supplier has provided a Test Specification in accordance with Paragraph 7 of Schedule 14 (Testing Procedures). - The Supplier has provided draft and final Test Report in accordance with Paragraph 8 of Schedule 14 (Testing Procedures). - The Supplier has provided a Test Report capable of Authority approval, in accordance with Schedule 14 Test Procedures, for all tests required to be carried out in respect of the establishment of the Soft LAN Services and the DMMP as documented in the	70 Working Days	Effective Date + 100 Working Days	Schedule and chair Service Readiness Review meetings	Not applicable

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	Test Strategy and Test Plans, including: ○ The Supplier DMMP integration is complete (e-bonding and operational monitoring integration with the Authority's ITSM Toolset). The Supplier Soft LAN Services support resources have been granted security clearance. ○ The Supplier has provided Soft LAN Services service management operational processes which are capable of Authority approval in accordance with Part B of this Schedule. ○ Soft LAN Services Supplier resource on boarding is complete. ○ Supplier confirmation that training of Supplier service management teams is complete (Schedule 14 Testing Procedures).				

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	○ Soft LAN Services service management processes and procedures testing is complete (including DMMP integration testing with the Authority ITSM Toolset). ○ Evidence that the Supplier DMMP meets the required Availability in accordance with Annex 1 Paragraph 11 (Availability) of Schedule 3(Performance Levels). • The Supplier has provided Product Descriptions for Documentary Deliverables for the next dependent Milestones. • The Supplier has achieved Milestone Achievement Certificate sign off for Milestones 1, 2, 3 and 4.				
M7 Security Sign Off – Documentary Deliverable	• The Supplier has provided an Information Management System (Schedule 5 Security Management) which is capable of Authority approval in accordance with Paragraph 4 of, Schedule 5.	70 Working Days	Effective Date + 110 Working Days	• Input into the scoping of the Supplier IT Health Check	Not applicable

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	• The Supplier has provided an Information Assurance Assessment (Schedule 5 Security Management) which is capable of Authority approval in accordance with Paragraph 6 of Schedule 5. • The Supplier has completed a Security IT Health Check (ITHC) (Schedule 5 Security Management) and produced a report in accordance with Paragraph 9 of Schedule 5. • The Supplier has provided security processes (Schedule 5 Security Management), these will be required to support the delivery of its Services. The security processes will be capable of Authority approval in accordance with Paragraph 7 of Schedule 5. • Certification Requirements evidenced in accordance with (Paragraph 8, Schedule 5 Security Management). • The Supplier has provided Product Descriptions for Documentary Deliverables for the next dependent Milestones.				
M8 Soft LAN Services Acceptance Sign Off	• Confirmation that the Soft LAN Services, Supplier Resource on boarding is complete.	5 Working Days	Effective Date + 115 Working Days	• Chair and schedule Service	ATP Milestone

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Non - Documentary Deliverable Second Operational Service Commencement Date	• The Supplier provided Authority approved ITSCM awareness and training for all their ITSCM related personnel (LAN Transition Requirements Schedule 2 Annex C). • The Supplier has provided the Authority with evidence which is capable of approval that they can operate the Soft LAN Services in line with the Schedule 3 (Performance Levels). • Achieved Operational Service Commencement Date for the Soft LAN Services, and provision of the Services to meet or exceed the Target Performance Levels for each relevant Performance Indicator. • The Supplier has achieved Milestone Achievement Certificate sign off for Milestones 6 and 7. • The Supplier has provided Product Descriptions for Documentary Deliverables for the next dependent Milestones: • "Gate Approval" of Gate 3 ('Build and Test') and Gate 4 ('Cutover to Service Commencement') as described			Readiness Review meetings.	The Supplier must have Achieved this Milestone 8 before it can commence provision of the relevant Operational Services Key Milestone (Y)

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	in the "Transition Framework" Standard.				
M9 – Pilot Site Acceptance Sign Off Non -Documentary Deliverable	• The Supplier has been issued with Site Transition Certificates by the Authority for the successful migration of the pilot Authority Sites. • Post Go Live Report: Approval Success: Quality Criteria to include: "as specified in requirements in Paragraph 7.1.2.5 of the Transition Requirements". • The Supplier has provided an Authority Site migration lesson learned report which is capable of Authority approval in accordance with Part B of this Schedule. • 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 Milestone 9.	5 Working Days	Effective Date + 120 Working Days	• Nominate pilot migration Authority Sites	The Supplier must have Achieved this Milestone 9 before it can commence provision of the relevant Operational Services

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	• The Supplier has been issued with a Milestone Achievement Certificate. • The Supplier has provided Product Descriptions for Documentary Deliverables for the next dependent Milestones. • "Gate Approval" of Gate 5 ('Handover to BAU') as described in the "Transition Framework" Standard.				
M10 - Fixed LAN and Wireless Services Transition Non -Documentary Deliverable Operational Services Commencement Date for Soft LAN Services Per Authority Site	Transition of the management of Fixed LAN and Wireless LAN infrastructure from the Preceding Services to the Operational Services, including (in respect of the Fixed LAN and Wireless LAN Services only) the provision of: • Cutover plan written and approved in accordance with Part B of this Schedule. • Management and support for all Devices and Licensed Software retained from the Preceding Services. • The Supplier has provided the Authority with evidence which is capable of approval that they can operate Services in line with the Schedule 3 (Performance Levels).	30 Working Days	Effective Date + 150 Working Days	Facilitate Supplier Site access requirements for the Soft LAN Services in line with the Authority Site access request process	Key Milestone (Y) ATP Milestone The Supplier must have Achieved this Milestone 10 before it can commence provision of the relevant Operational Services.

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	• The Supplier has provided a LAN Authority Site migration plan which is capable of Authority approval in accordance with Part B of this Schedule. • 100% Supplier take on of the fixed LAN and wireless LAN infrastructure of the Authority System complete in accordance with Technical Requirements Schedule 2 Annex B. • 100% LAN Authority Sites transitioned into Business as Usual (BAU) support in accordance with Paragraph 7.1.2.10 (LAN Transition Requirements Schedule 2 Annex C). • 100% Supplier take on of the NAC solutions used by the Authority in accordance with Paragraph 2.4.2 (Technical Requirements Schedule 2 Annex B). • 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				

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	each relevant Performance Indicator. Site Transition Certificates issued for all Authority Sites in Milestone 10. • The Supplier has completed Site Low-Level Designs. These will include: - Detailed physical layer topology diagrams including depicting physical devices, its interface connection uplinks (to other network devices such as switches, wireless access points, routers, firewalls etc.), Spanning-Tree topologies where applicable etc. - Detailed logical layer topology diagrams including depicting routed topology, VLAN, Layer 3 IP information etc. - Site communications rooms cabling diagrams and configurations of LAN supported devices at the site • “Gate Approval” of Gate 5 (‘Handover to BAU’) as described in the “Transition Framework” Standard.				

ANNEX 1: (Outline Implementation Plan)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

M11 – Transition Complete Non -Documentary Deliverable	• The Supplier has achieved Milestone Achievement Certificates sign off for Milestones 8, 9 and 10. • Transition Closure Report: Approval Success: Quality Criteria to include: “as specified in requirements in Paragraph 7.1.2.16 of the Transition Requirements”. • “Gate Approval” of Gate 6 (‘Transition Complete’) as described in the “Transition Framework” Standard.	10 Working Days	Effective Date + 160 Working Days	Not applicable	CPP Milestone (Y) Key Milestone (Y)

**ANNEX 2: (Format for Product Descriptions for
Documentary Deliverables)**

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

**ANNEX 2: FORMAT FOR PRODUCT DESCRIPTIONS FOR DOCUMENTARY
DELIVERABLES**

<u>PRODUCT 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	

ANNEX 3: EXISTING PRODUCT DESCRIPTIONS

<u>PRODUCT</u> <u>REFERENCE</u>	<i>[For internal use only]</i>
Title of Deliverable	Detailed Implementation Plan - LAN
Purpose of Deliverable	To document how the Supplier and its Sub-contractors shall comply with the requirements set out below and the Contract, when implementing its Operational Services to support the Authority LAN services. • Schedule 3 (performance Levels) • Schedule 5 (Security Management) • Schedule 13 (Implementation Plan) • Schedule 14 (Testing Procedures) • Schedule 26 (Service Continuity Plan and Corporate Resolution Planning) • Service Management Requirements • Technical Requirements • Transition Requirements
Format & Presentation of Deliverable	Microsoft Word Document and Microsoft Project
Project or Programme	LAN
Scope of Deliverable	Operational Services
Composition of Deliverable	As described in Paragraph 3 of Schedule 13 (Implementation Plan) but not limited to.
Derivation of Deliverable	• Supplier / Authority Workshops • Schedule 3 (performance Levels) • Schedule 5 (Security Management) • Schedule 13 (Implementation Plan) • Schedule 14 (Testing Procedures) • Schedule 26 (Service Continuity Plan and Corporate Resolution Planning) • Service Management Requirements • Technical Requirements • Transition Requirements • Preceding supplier designs
Allocated to	Supplier
Quality Criteria for Deliverable	Contains all required content in accordance with Schedule 13 (Implementation Plan).

ANNEX 3: (Existing Product Deliverables)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Quality Method	The Authority will check that the Detailed Implementation contains all the required content. For the avoidance of doubt, acceptance of the Documentary Deliverable will be in accordance with Paragraph 3 and Part B of Schedule 13 (Implementation Plan).
People or skills required	
First Draft Delivery Date for Deliverable	In accordance with the approved Detailed Implementation Plan
Planned Successful Approval Date for Deliverable	In accordance with the approved Detailed Implementation Plan

<u>PRODUCT REFERENCE</u>	<i>[For internal use only]</i>
Title of Deliverable	High Level Design (HLD) - LAN
Purpose of Deliverable	To document how the Supplier and its Sub-contractors shall comply with the requirements set out below and the Contract, when delivering its Operational Services to support the Authority LAN services. • Schedule 3 (performance Levels) • Schedule 5 (Security Management) • Schedule 13 (Implementation Plan) • Schedule 26 (Service Continuity Plan and Corporate Resolution Planning) • Service Management Requirements • Technical Requirements • Transition Requirements
Format & Presentation of Deliverable	Microsoft Word Document and Microsoft Visio diagrams
Project or Programme	LAN
Scope of Deliverable	Operational Services
Composition of Deliverable	The HLD should include, but not be limited to: System Overview\ Architecture: A description of the overall structure of the solution being proposed by the Supplier to manage and monitor the Authority LAN services, including the main components and their relationships. Network Architecture: Document, at high level the proposed solution and the component deployment patterns which will be used to deliver the Operational Services to support the Authority LAN services providing the rationale for implementation patterns. Not limited to: • Sites • Network Segments Product Design Specification: A description of the Device Monitoring Management Platform (DMMP), features, functionalities, and design considerations.

	Data \ Network Traffic Flow: Detail how network data will flow through the LAN, ITSM tooling, including inputs, outputs, and data processing steps. Including how the Supplier solution will connect to the Authority network. Interfaces: Describes the interfaces between different components or systems, including APIs, protocols, and communication methods. This ensures interoperability and defines how the Supplier systems will interface with the IT Environment. Design Scope and Exclusions: Document the boundaries of the design and provide context for this. Design Constraints: Limitations or restrictions in the design imposed by internal and external factors. Solution Components: Details of the key components and most significant features that provide the Supplier solution, including. Not limited to: • Physical or Logical Infrastructure Components • Integration of the Solution • Support and Management Tooling • System Access • System Management Interfaces: A description of the solution interfaces including traffic/protocols or transport and communication methods. Not limited to: • Authority systems • Interfaces with the Authority LAN services. • End user access. • Reporting • Capacity management • Remote Access • System administration • Management • Patching • Monitoring • Security event management • IDAM • Backup systems • Network Service Integration – NTP/DNS/DHCP

	Security: Articulate high-level strategies for securing the Supplier's solution to meet the Authority requirements. Not limited to: • Authentication • Authorisation • Encryption • Data management • Data protection measures Business Continuity and Availability: Articulate high-level strategies the Supplier solution and its components utilise to maintain availability and support disaster recovery objectives. Dependencies: Document external dependencies and integrations with other systems or services needed to fulfil the requirements of Supplier solution. Integration: Identifies external integration points with other systems or services, for example; the Authority ITSM. APIs, Management Information Systems. RAID: Detail risks, assumptions, issues, and dependencies associated with the implementation of the proposed High-Level Design.
Derivation of Deliverable	• Supplier / Authority Workshops • Schedule 3 (performance Levels) • Schedule 5 (Security Management) • Schedule 13 (Implementation Plan) • Schedule 26 (Service Continuity Plan and Corporate Resolution Planning) • Service Management Requirements • Technical Requirements • Transition Requirements • Preceding supplier designs
Allocated to	Supplier
Quality Criteria for Deliverable	Contains all required content in accordance with: - • Service Management Requirements • Technical Requirements • Schedule 13 (Implementation Plan)
Quality Method	The Authority will check that the High-Level Design contains all the required content.

ANNEX 3: (Existing Product Deliverables)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	For the avoidance of doubt, acceptance of the Documentary Deliverable will be in accordance with Part B of Schedule 13 (Implementation Plan).
People or skills required	
First Draft Delivery Date for Deliverable	In accordance with the approved Detailed Implementation Plan
Planned Successful Approval Date for Deliverable	In accordance with the approved Detailed Implementation Plan

<u>PRODUCT REFERENCE</u>	<i>[For internal use only]</i>
Title of Deliverable	High Level Service Design
Purpose of Deliverable	To document how the Supplier and its Sub-contractors shall comply with the requirements set out below and the Contract, when delivering its Operational Services to support the Authority LAN services. • Schedule 3 (performance Levels) • Schedule 5 (Security Management) • Schedule 13 (Implementation Plan) • Schedule 26 (Service Continuity Plan and Corporate Resolution Planning) • Service Management Requirements • Technical Requirements • Transition Requirements
Project or Programme	LAN
Scope of Deliverable	Operational Services
Format & Presentation of Deliverable	Microsoft Word Document and Microsoft Visio diagrams
Composition of Deliverable	Service Description: An overview of the Operational Services including the characteristics and features, this will include: - • Service Overview - Summary of the target Operational Services and their purpose. Also, how they meet the business case objectives of the Authority. • Service Scope – The service boundaries of the Supplier's Operational Services, including what is within the Supplier support scope and what is out of scope. E.g. services are out of scope for the Supplier Operational Services. • Service Objectives – Objectives of the Operational Services and alignment to target availability and performance measures. • Service Components – Detail the components that make up the service e.g. hardware, ITSM tooling, service processes, security processes and any other resources involved in delivering the Operational Services.

	• Service Levels and KPI's – Detail the target Service Levels and KPI's associated with the Operational Services. • Service Dependencies – Identify any dependencies the Operational Services will have on other service components or services e.g. access to the Authority ITSM system and other network services such as DNS, DHCP etc. • Service Delivery Processes – Description as to how the service is delivered, including any processes, workflows, or procedures that are followed to deliver the Operational Services. • Service Support Process – Description as to how support for the service is provided for the Operational Services, including how incidents, problems, and service requests are handled. This will detail how the Supplier will integrate with the Authority's service management capabilities. • Supplier Management: Description how the Supplier will manage its Supplier's to ensure that they meet the agreed Service Levels and applicable requirement flow downs.
Derivation of Deliverable	• Supplier / Authority Workshops • Schedule 3 (performance Levels) • Schedule 5 (Security Management) • Schedule 13 (Implementation Plan) • Schedule 26 (Service Continuity Plan and Corporate Resolution Planning) • Service Management Requirements • Technical Requirements • Transition Requirements • Preceding supplier designs
Allocated to	Supplier
Quality Criteria for Deliverable	Contains all required content in accordance with: - • Service Management Requirements • Technical Requirements • Schedule 13 (Implementation Plan)
Quality Method	The Authority will check that the High-Level Service Design contains all the required content. For the avoidance of doubt, acceptance of the Documentary Deliverable will be in accordance with Part B of Schedule 13 (Implementation Plan).

ANNEX 3: (Existing Product Deliverables)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

People or skills required	Security Architect Service Architect Technical Architect Service Operations
First Draft Delivery Date for Deliverable	TBC confirmed by the Supplier
Planned Successful Approval Date for Deliverable	TBC confirmed by the Supplier

<u>PRODUCT REFERENCE</u>	
Title of Deliverable	Low Level Design (LLD) – LAN
Purpose of Deliverable	To document how the Supplier and its Sub-contractors shall comply with the requirements set out below and the Contract, when delivering its Operational Services to support the Authority LAN services. • Schedule 3 (performance Levels) • Schedule 5 (Security Management) • Schedule 13 (Implementation Plan) • Schedule 26 (Service Continuity Plan and Corporate Resolution Planning) • Service Management Requirements • Technical Requirements • Transition Requirements
Project or Programme	LAN
Scope of Deliverable	Operational Services
Format & Presentation of Deliverable	Microsoft Word Document and Microsoft Visio diagrams
Composition of Deliverable	The LLD must include, but not limited to: Design background: Document the purpose and outcomes the design supports. Design scope summary: Document design exclusions and inclusions to inform the boundaries of the design. Design constraints: List the limitations or restrictions in the design imposed by internal and external factors. System architecture: Document the detailed structure of the solution, including but limited to the DMMP. Network and data traffic flow: Detail how network data will flow through the LAN, including inputs, outputs, and data processing steps. Including how the Supplier solution will connect to the Authority network. Network services (e.g. DNS, DHCP, NTP etc.): Detailed configuration of network services and how they will be implemented. Device Management and Monitoring – Configuration details of the Device Management and Monitoring Platform.

	Which enable the monitoring and management of the Authority LAN services. Security architecture: Detail security configurations, including firewall rules, ACLs, and network segmentation. Backup and recovery: Detail backup and recovery procedures, including schedules and tools to be used. Site configurations – Site LAN configuration details including but not limited to: • Logical layer topology diagrams including depicting routed topology, VLAN, Layer 3 IP information etc. • Site communications rooms cabling diagrams and configurations of LAN supported devices at the Site. Interfaces: Document the interfaces of components of the solution including traffic/protocols or transport and communication methods. Not limited to: • Management • Monitoring • Access • Authentication • Data controls • Protocols and transport Security: Document configuration or integration used for securing the Supplier solution and its components to meet the Supplier's requirements. Not limited to: • Access Control List (ACL) • Authentication • Authorisation • Security monitoring and compliance • Vulnerability management • External system security • Encryption • Data management • Data protection measures Business Continuity and Availability: Document how the Supplier solution and its components maintain availability and support disaster recovery objectives. Include SLA's and designed availability.

	Integration: Specific configuration of integration points of the Supplier solution with other systems and services. Not limited to: • Authority system's • Certificate services • System access for administration • System access for end users • Reporting configuration • Capacity management • Remote access • Management integration • Patching • Monitoring • Security Event Management • IDAM • System backup • Network service - NTP/DNS/DHCP • Automation Dependencies: Document external dependencies and integrations with other systems or services needed to fulfil the requirements of Supplier solution. RAID: Detail risks, assumptions, issues, and dependencies associated with the design.
Derivation of Deliverable	• Supplier / Authority Workshops • Schedule 3 (performance Levels) • Schedule 5 (Security Management) • Schedule 13 (Implementation Plan) • Schedule 26 (Service Continuity Plan and Corporate Resolution Planning) • Service Management Requirements • Technical Requirements • Transition Requirements • Preceding supplier designs
Allocated to	Supplier
Quality Criteria for Deliverable	Contains all required content in accordance with: - • Technical Requirements • Schedule 3 (Performance Levels) • Schedule 5 (Security Management) • Schedule 13 (Implementation Plan) • Schedule 26 (Service Continuity Plan and Corporate Resolution Planning)
Quality Method	The Authority will check that the Low-Level Design contains all the required content.

ANNEX 3: (Existing Product Deliverables)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	For the avoidance of doubt, acceptance of the Documentary Deliverable will be in accordance with Part B of Schedule 13 (Implementation Plan).
People or skills required	
First Draft Delivery Date for Deliverable	In accordance with the Detailed Implementation Plan
Planned Successful Approval Date for Deliverable	In accordance with the Detailed Implementation Plan

<u>PRODUCT REFERENCE</u>	<i>[For internal use only]</i>
Title of Deliverable	Low Level Service Design
Purpose of Deliverable	To document how the Supplier and its Sub-contractors shall comply with the requirements set out below and the Contract, when delivering its Operational Services to support the Authority LAN services. • Schedule 3 (performance Levels) • Schedule 5 (Security Management) • Schedule 13 (Implementation Plan) • Schedule 26 (Service Continuity Plan and Corporate Resolution Planning) • Service Management Requirements • Technical Requirements • Transition Requirements
Project or Programme	LAN
Scope of Deliverable	Service Components: Detailed specifications of each component of the Operational Services, including hardware, software and ITSM tooling etc. Interfaces: Detail how different components of the services will interact with each other and with external systems or other Authority services. Capacity planning: details the resources required to support the services. Security design: Aligns the baseline security requirements and how the appropriate measures will be undertaken to protect the Authority LAN and its data. Availability: Detailing how the Operational Services will meet the availability targets e.g. through redundancy, disaster recovery etc. IT Service Continuity Management: Detail as to how the Operational Services can be recovered and restored in the event of a disaster or other disruptive event. Information Security Management: Detail how the LAN Services and systems are protected from unauthorised access, breaches, and other security threats including any details of accreditation and certification e.g. ISO27001.

ANNEX 3: (Existing Product Deliverables)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Format & Presentation of Deliverable	Microsoft Word Document and Microsoft Visio diagrams
Composition of Deliverable	As described in: - • Service Management Requirements • Technical Requirements • Schedule 3 (Performance Levels) • Schedule 13 (Implementation Plan)
Derivation of Deliverable	• Supplier / Authority Workshops • Schedule 3 (performance Levels) • Schedule 5 (Security Management) • Schedule 13 (Implementation Plan) • Schedule 26 (Service Continuity Plan and Corporate Resolution Planning) • Service Management Requirements • Technical Requirements • Transition Requirements • Preceding supplier designs
Allocated to	Supplier
Quality Criteria for Deliverable	As described in: - • Service Management Requirements • Transition Requirements • Schedule 13 (Implementation Plan)
Quality Method	The Authority will check that the Low-Level Service Design contains all the required content. For the avoidance of doubt, acceptance of the Documentary Deliverable will be in accordance with Part B of Schedule 13 (Implementation Plan).
People or skills required	
First Draft Delivery Date for Deliverable	In accordance with the Detailed Implementation Plan
Planned Successful Approval Date for Deliverable	In accordance with the Detailed Implementation Plan

ANNEX 3: (Existing Product Deliverables)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

<u>PRODUCT REFERENCE</u>	[For internal use only]
Title of Deliverable	Security Management Plan
Purpose of Deliverable	To document how the Supplier and its Sub-contractors shall comply with the requirements set out in Schedule 5 (Security Management) and the Contract in order to ensure the security of the Authority Data and the Information Management System.
Project or Programme	LAN
Scope of Deliverable	Information Management System \ CIMS \ WIMS
Format & Presentation of Deliverable	Template provided in Annex 3 of Schedule 5 (Security management).
Composition of Deliverable	As described in Annex 3 of Schedule 5 (Security management).
Derivation of Deliverable	Supplier to produce, in accordance with Schedule 5.
Allocated to	Supplier
Quality Criteria for Deliverable	Contains all required content in accordance with Schedule 5 (Security Management).
Quality Method	• The Authority will check that the SMP contains all the required content. • For the avoidance of doubt, acceptance of the Documentary Deliverable shall be in accordance with the provisions of Paragraph 7 of Schedule 5.
People or skills required	
First Draft Delivery Date for Deliverable	In accordance with the Detailed Implementation Plan
Planned Successful Approval Date for Deliverable	In accordance with the Detailed Implementation Plan

<u>PRODUCT REFERENCE</u>	
Title of Deliverable	Solution Design – LAN
Purpose of Deliverable	To document how the Supplier and its Sub-contractors shall comply with the requirements set out below and the Contract, when delivering its Operational Services to support the Authority LAN services. • Schedule 3 (performance Levels) • Schedule 5 (Security Management) • Schedule 13 (Implementation Plan) • Schedule 26 (Service Continuity Plan and Corporate Resolution Planning) • Service Management Requirements • Technical Requirements • Transition Requirements
Project or Programme	
Scope of Deliverable	Operational Services
Format & Presentation of Deliverable	Microsoft Word Document and Microsoft Visio diagrams
Composition of Deliverable	The Solution Design must include, but not be limited to: Background: Provides context and an overview of the project's objectives. Executive Summary: Summarises the Solution Design's key points and goals. Objectives: Outlines the components, architecture, and functionality of a solution to address the Authority requirements across both the contract schedules and statement of requirements. This document will provide a narrative summary of the end-to-end solution and how it interfaces with Authority's LAN and other services. The Solution Design will provide a single documentary deliverable detailing and defining all components of the Supplier solution in delivering its Operational Services Service Requirements: Demonstrates alignment of the Authority service objectives that the solution aims to address for the Authority. Architecture Overview: Describes the high-level vision of the proposed solution, including scope and context.

	Technology Baseline: Documents the existing technology and systems before implementing the new solution. Architectural Strategy: Explains the chosen architectural approach, methodologies, models, and tools. System Architecture: Provides detailed diagrams and descriptions of hardware, software, networks, and data structures. Infrastructure Architecture: Outlines necessary physical and virtual resources that will provide the solution. Security Architecture: Specify how the service will be protected and compliant with security standards. Service Architecture: Specify how the solution will meet the service requirements of the Authority. Integration and Data Flow: Describes data flow within the system and integration with other systems. Non-Functional Requirements: Specifies operational characteristics (e.g., performance, reliability, scalability). Transition and Migration Plan: Includes strategies for transitioning to the new system, including data migration. RAID (Risks, Assumptions, Issues, Dependencies): Document risks, assumptions, issues, and dependencies related to the Supplier solution implementation.
Derivation of Deliverable	• Supplier / Authority Workshops • Schedule 3 (performance Levels) • Schedule 5 (Security Management) • Schedule 13 (Implementation Plan) • Schedule 26 (Service Continuity Plan and Corporate Resolution Planning) • Service Management Requirements • Technical Requirements • Transition Requirements • Preceding supplier designs
Allocated to	Supplier
Quality Criteria for Deliverable	Contains all required content in accordance with: - • Service Management Requirements • Technical Requirements • Transition Management • Schedule 3 (performance Levels)

ANNEX 3: (Existing Product Deliverables)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	• Schedule 5 (Security Management) • Schedule 13 (Implementation Plan) • Schedule 26 (Service Continuity Plan and Corporate Resolution Planning)
Quality Method	The Authority will check that the Solution Design contains all the required content. For the avoidance of doubt, acceptance of the Documentary Deliverable will be in accordance with Part B of Schedule 13 (Implementation Plan).
People or skills required	
First Draft Delivery Date for Deliverable	In accordance with the Detailed Implementation Plan
Planned Successful Approval Date for Deliverable	In accordance with the Detailed Implementation Plan

ANNEX 3: (Existing Product Deliverables)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

<u>PRODUCT REFERENCE</u>	[For internal use only]
Title of Deliverable	Test Strategy
Purpose of Deliverable	To document how the Supplier and its Sub-contractors shall comply with the requirements set out in Schedule 14 (Testing Procedures) and the Contract in order to assure the delivery of the Operational Services in accordance with the Authority Requirements.
Project or Programme	LAN
Scope of Deliverable	Operational Services
Format & Presentation of Deliverable	Microsoft Word document
Composition of Deliverable	As described in Schedule 14 (Testing Procedures)
Derivation of Deliverable	Supplier to produce, in accordance with Schedule 14
Allocated to	Supplier
Quality Criteria for Deliverable	Contains all required content in accordance with Schedule 14 (Testing Procedures)
Quality Method	• The Authority will check that the Test Strategy contains all the required content. • For the avoidance of doubt, acceptance of the Documentary Deliverable will be in accordance with Part B of Schedule 13 (Implementation Plan).
People or skills required	
First Draft Delivery Date for Deliverable	In accordance with the Detailed Implementation Plan
Planned Successful Approval Date for Deliverable	In accordance with the Detailed Implementation Plan

SCHEDULE 14 (Testing Procedures)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 14
Testing Procedures

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: (h) for the Testing of Non-Documentary Deliverables; and (i) 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

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 and/or a conditional Milestone Achievement Certificate shall not:

- (a) operate to transfer any risk that the relevant Deliverable or Milestone is complete or will meet and/or satisfy the Authority's requirements for that Deliverable or Milestone; or
- (b) affect the Authority's right subsequently to reject:
 - (i) all or any element of the Deliverables to which a Test Certificate relates; or
 - (ii) any Milestone to which the Milestone Achievement 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.

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;
 - (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.

- 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 provided that the Parties agree that Test data shall be provided from a non-production environment and any Personal Data shall be redacted so that it cannot be traced or identified;
- (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.

SCHEDULE 14 (Testing Procedures)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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.
- 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.

SCHEDULE 14 (Testing Procedures)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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.
- 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;
- (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.
- 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 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.

SCHEDULE 14 (Testing Procedures)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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:
- (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

SCHEDULE 14 (Testing Procedures)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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);
 - (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 or Authority Sites.
- 14.4 The Supplier must comply with Paragraph 14.1(b) in relation to each Authority Site but for the avoidance of doubt, the Supplier may submit the required evidence for more than one Authority Site at the same time.

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

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]**

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]**

ANNEX 4: TEST SUCCESS CRITERIA**1 Tests to be Achieved in order to Achieve the ATP Milestones**

ATP Milestone Name	Test	Pre-conditions*	Test Success Criteria
M5 - Hard LAN services acceptance sign off	Supplier operational support processes for the Hard LAN services	- The Authority has signed off against the Supplier High-Level Design and Hard LAN services Service Design Package - Supplier training has completed	The Supplier can evidence that it can support the Hard LAN services against the Service Levels (Schedule 3 Performance Levels) The Supplier can evidence that it can manage Hard LAN services incidents against the Service Levels (Schedule 3 Performance Levels) The Supplier can evidence that it can manage Hard LAN services, requests against the Service Levels (Schedule 3 Performance Levels)
	Supplier operational processes integrate with the Authority's service management processes	Authority ITIL processes have been shared with the Supplier	Supplier can evidence that it can integrate with the Authority's service management processes to support the Hard LAN services against the Service Levels (Schedule 3 Performance Levels)
M8 Soft LAN services acceptance sign off	Supplier operational support processes for the Soft LAN services	- The Authority has signed off against the Supplier's High-Level Design and Soft LAN services Service Design Package - The Supplier will have achieved it's Success Criteria for milestone M6 – Soft LAN Services testing sign off - The Supplier will have achieved it's Success	The Supplier can evidence that it can support the Soft LAN services against the Service Levels (Schedule 3 Performance Levels) The Supplier can evidence that it can manage Soft LAN services incidents against the Service Levels (Schedule 3 Performance Levels) The Supplier can evidence that it can manage Hard LAN services, requests against the Service Levels (Schedule 3 Performance Levels)

ANNEX 4: (Test Success Criteria)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

		Criteria for milestone M7 security sign off	
	Supplier operational processes integrate with the Authority's service management processes	- Authority ITIL processes have been shared with the Supplier - The Supplier will have achieved it's Success Criteria for milestone M6 – Soft LAN Services testing sign off - The Supplier will have achieved it's Success Criteria for milestone M7 security sign off	Supplier can evidence that it can integrate with the Authority's service management processes to support the Soft LAN services against the Service Levels (Schedule 3 Performance Levels)
M10 - Fixed LAN and Wireless services transition	- Supplier can proactively manage fixed LAN services for the Authority Site - Supplier can proactively manage the wireless LAN services for the Authority Site	- The Supplier will have achieved it's Success Criteria for milestone M8 Soft LAN services acceptance sign off - The Supplier will have achieved it's Success Criteria for milestone M9 – Pilot site acceptance sign off	100% Supplier take on of the Preceeding fixed LAN and wireless LAN Services complete in accordance with Technical Requirements Schedule 2 Annex B 100% LAN Authority Sites transitioned into Business as Usual (BAU) support in accordance with Paragraph 7.1.2.10 (LAN Transition Requirements Schedule 2 Annex C) 100% Supplier take on of the NAC solutions used by the Authority in accordance with Paragraph 2.4.2 (Technical Requirements Schedule 2 Annex B)

ANNEX 4: (Test Success Criteria)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

*** Note:** *The Pre-Conditions are that e.g. the Success Criteria for the previous Tests must be satisfied before the ATP Milestone tests are commenced*

2 Tests to be Achieved in order to Achieve a CPP Milestone

CPP Milestone Charge No.	Test	Test Success Criteria
M11 – Transition Complete	• Lessons learned report sign off • Transition closure report sign off	• The Supplier has achieved Milestone Achievement Certificates sign off for Milestones 8, 9 and 10

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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(s)]**

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(s)]** 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(s)]** is: **[insert date of this certificate]**.

Yours faithfully

[Name]

[Position]

acting on behalf of **[name of Authority]**

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 15
CHARGES AND INVOICING

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;
“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 in Great Britain” as published by the Office for National Statistics;
“Catalogue Item Charges”	has the meaning given to it in Paragraph 3.4 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>);
“Consumed”	means: (a) in respect of time and materials resource, the 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:

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN 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 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

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 Rate”

has the meaning given in Paragraph 1.1(a) of PART C (*Adjustments to the Charges and Risk Register*) of this Schedule 15;

“The Employer Pension Contributions”

means:

- (a) in respect of CSPA 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;
- (b) in respect of NHSPA 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,

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

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';

“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 to it 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 3.2 of Part A (*Pricing*) of this Schedule 15;

“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);

“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

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	(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 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>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 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;
"Maximum Permitted Profit Margin"	the Anticipated Contract Life Profit Margin plus 5%;
"Milestone Group"	has the meaning given in Paragraph 3.6 of Part B (<i>Project Charges</i>) 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 (<i>Adjustments to the Charges and Risk Register</i>) of this Schedule 15;

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

“Monthly Service Charges”	has the meaning given in Paragraph 3.3 of Part A (<i>Pricing</i>) 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;
“Payment Planner”	means a report provided by the Supplier in respect of each Service Period to the Authority containing information on historical and forecast consumption and the associated Charges;
“Reconciliation Report”	has the meaning given in Paragraph 8.6 of Part C (<i>Adjustments to the Charges and Risk Register</i>) 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 3 of Part A (<i>Pricing</i>) of this Schedule 15;

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

“Service Credit Cap”	has the meaning given in Paragraph 3.2 of Part C (<i>Adjustments to the Charges and Risk Register</i>) of this Schedule 15;
“Service Credit Point Value”	means the value for each Service Point as calculated in accordance with Paragraph 3.8 of Part C (<i>Adjustments to the Charges and Risk Register</i>) 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 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;
“Volume Based Service Charges”	has the meaning given to it in Paragraph 3.3 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

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 2 of this Part A;

1.1.2 the Service Charges payable in accordance with Paragraph 3 of this Part A; and

1.1.3 Project Charges payable in accordance with Part B (*Project Charges*) of this Schedule 15.

2 MILESTONE PAYMENTS

2.1 The Milestone Payments are charged on a fixed price basis and are set out in the table in Annex A (*Milestone Payments and Delay Payments*) to this Schedule 15.

2.2 Subject to the provisions of Part C (*Adjustments to the Charges and Risk Register*) of this Schedule 15 in relation to the deduction of Delay Payments for Key Milestones and provided the Authority has issued a Milestone Achievement Certificate in respect of all previous Milestones, on the Achievement of a Milestone (for the avoidance of doubt including Key Milestones) the Supplier shall be entitled to invoice the Authority for the Milestone Payment associated with that Milestone less the applicable Milestone Retention.

2.3 Each invoice relating to a Milestone Payment shall be supported by a Milestone Achievement Certificate and all relevant Supporting Information.

2.4 The Milestone Payments shall not be subject to Indexation.

Release of Milestone Retentions

2.5 On Achievement of the CPP Milestone (Milestone 11 (Transition Complete)), the Supplier shall be entitled to invoice the Authority for an amount equal to the sum of all Milestone Retentions that relate to Milestones identified in the Implementation Plan for which a Milestone Achievement Certificate has been issued and have been paid before Achievement of such Milestone 11 (Transition Complete) less any Delay Payments deducted in accordance with Paragraph 3 of Part C (*Adjustments to the Charges and Risk Register*) of this Schedule 15.

3 SERVICE CHARGES

3.1 The Service Charges shall be payable by the Authority to the Supplier and shall comprise:

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 3.1.1 the **Fixed Service Charges** (calculated in accordance with Paragraph 3.2 below; and
 - 3.1.2 the **Volume Based Service Charges** calculated in accordance with Paragraph 3.3 below; and
 - 3.1.3 the **Catalogue Item Charges** (calculated in accordance with Paragraph 3.4 below).
- 3.2 Fixed Service Charges
- 3.2.1 The Fixed Service Charges payable by the Authority are set out in Paragraph **Error! Reference source not found.** of Annex B (*Service Charges*) to this Schedule 15 and shall comprise:
 - (a) **Hard LAN Services – Service Management Charges** payable with effect from the First Operational Service Commencement Date (Achievement of Milestone 5); and
 - (b) **Soft LAN Services – Service Management Charges** payable with effect from the Second Operational Service Commencement Date (Achievement of Milestone 8).
 - 3.2.2 The Supplier shall be entitled to Index the Fixed Service Charges in accordance with Part C (*Adjustments to the Charges and Risk Register*) of this Schedule 15.
- 3.3 Volume Based Service Charges
- 3.3.1 The Volume Based Service Charges payable by the Authority are set out in Annex C (*Volume Based Service Charges*) to this Schedule 15 and shall comprise:
 - (a) **Hard LAN Services – Variable Run and Maintain Charges** payable with effect from the First Operational Service Commencement Date (Achievement of Milestone 5); and
 - (b) **Soft LAN Services – Variable Run and Maintain Charges** payable with effect from the Second Operational Service Commencement Date (Achievement of Milestone 8).
 - 3.3.2 The Supplier shall be entitled to Index the Volume Based Service Charges in accordance with Part C (*Adjustments to the Charges and Risk Register*) of this Schedule 15.
 - 3.3.3 The Parties agree that the closure of an Authority Site or a reduction in the number of Devices 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, 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 Devices.

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

3.4 Catalogue Item Charges

- 3.4.1 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.
- 3.4.2 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 of Annex B (*Service Charges*) to this Schedule 15.
- 3.4.3 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.
- 3.4.4 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).
- 3.4.5 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;
 - (e) delivery location;
 - (f) allocation/business unit/cost centre/entity code;

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (g) item code;
 - (h) item description; and
 - (i) net amount;
- 3.4.6 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).
- 3.4.7 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.
- 3.4.8 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 3.4.7 and this Paragraph 3.4.8 shall not be applied retrospectively or back-dated.
- 3.4.9 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.
- 3.4.10 Optional charges for support, warranty and/or refresh of a Catalogue Item shall be determined by agreement between the Parties where applicable.

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- 3.4.11 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 3.4.13, 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.
- 3.4.12 If the Authority exercises either of its options pursuant to Paragraph 3.4.11, 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.
- 3.4.13 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.
- 3.4.14 The Supplier shall not be entitled to add any costs, other than those listed at Paragraph 3.4.9 above, to the charges for Catalogue Items.
- 3.4.15 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.
- 3.4.16 If the Authority purchases assets, materials, software and equipment from the Product and Services Catalogue, then these shall be deemed to be Authority Assets.

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 3.4.17 For the avoidance of doubt, the Catalogue Item Charges shall not be subject to Indexation.

4 CALCULATION OF MONTHLY SERVICE CHARGES

- 4.1 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.
- 4.2 If a Service Charge:
- 4.2.1 commences on a day other than the first day of a month; and/or
 - 4.2.2 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.
- 4.3 The Service Charges for each Service Period ("**Monthly Service Charges**") shall be the aggregate of:
- 4.3.1 the Fixed Service Charges for the relevant Service Period; and
 - 4.3.2 the Volume Based Service Charges for the relevant Service Period; and
 - 4.3.3 the Catalogue Item Charges for the relevant Service Period.
- 4.4 The Supplier acknowledges and agrees that the Authority gives no warranty or representation as to:
- 4.4.1 the volume of Operational Services; and/or
 - 4.4.2 the total Service Charges.

Service Credits

- 4.5 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.
- 4.6 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

5 TIME AND MATERIAL CHARGES

- 5.1 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):

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 5.1.1 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; and
- 5.1.2 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.
- 5.2 The Supplier shall be entitled to Index the rates set out in table 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.
- 6 REIMBURSABLE EXPENSES**
- 6.1 The Charges (including the Milestone Payments, Fixed Service Charges, Volume Based Service Charges, Catalogue Item 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:
- 6.1.1 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
 - 6.1.2 any amount for any Services provided or costs incurred by the Supplier prior to the Commencement Date.
- 6.2 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

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Authority has approved such expenses in writing prior to the expenses being incurred and provided that such Reimbursable Expenses are supported by Supporting Documentation.

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 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 5 of Part A (*Pricing*) of this Schedule 15 will apply; or
 - 1.2.4 Catalogue Item Charges, in which event Paragraph 3.4 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 in the relevant Project Work Order. Payment shall be made to the Supplier in accordance with Part E (*Invoicing and Payment Terms*) of this Schedule 15.

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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:

$$\text{Milestone Payment} = TP - ((TC - IC)/2)$$

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) $IC > TC$; and

(ii) $TP + ((IC - TC)/2) < GMP$,

then Milestone Payment = $TP + ((IC - TC)/2)$; or

(b) if:

(i) $IC > TC$; and

(ii) $TP + ((IC - TC)/2) \geq GMP$,

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 relevant Milestone, less the Milestone Retention calculated using such Target Price, upon the issue of the associated Milestone Achievement Certificate; and

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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.

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**”) of 1/60th of 20% of the Milestone Payment for the relevant Key Milestone;
- (b) from (but excluding) the relevant Milestone Date to (and including) the later 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.

1.2 The Key Milestones are:

- 1.2.1 Key Milestone 5 – First Operational Service Commencement Date
- 1.2.2 Key Milestone 8 – Second Operational Service Commencement Date
- 1.2.3 Key Milestone 10 – Fixed LAN and Wireless Services Transition.

1.3 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, within 5 Working Days, issue a credit note to the Authority in respect of the relevant amount.

1.4 Any amounts credited to the Authority pursuant to Paragraph 3 shall not be refundable to the Supplier in any circumstances, including where a Delay as referred to in the Supplier’s notice:

- (a) does not occur; or
- (b) does occur but continues for fewer days during the relevant Delay Deduction Period than the number of days referred to in the Supplier’s notice.

1.5 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.

1.6 The Delay Payment in respect of a Key Milestone (net of any payment made in respect of that Key Milestone pursuant to Paragraph 3) shall be shown as a

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 3); and
- (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:

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

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 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

(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 Paragraphs 3.5 to 3.10 below and by reference to the number of applicable Service Points accrued in any one Service Period pursuant to the provisions of Schedule 3 (Performance Levels).

3.1.1 Illustrative examples of Service Credit calculations for KPIs 09 and 10 are set out in Annex H (Illustration of Service Points Accrual and Service Credits) to this Schedule 15 (Charges and Invoicing).

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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). **“Service Credit Cap”** shall mean:

- (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, 20% of the Monthly Service Charges; and
- (b) for each Service Period falling within the remainder of the Term, 35% of the Monthly Service Charges.

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.

Operational KPIs 01 to 07

3.5 The Service Credit due in respect of each Operational KPI (KPIs 01 to 07) 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 Paragraphs 1 to 10 of Annex 1, Part B of Schedule 3 (Performance Levels); and
- B is the applicable percentage deduction, being either:
 - (i) 0.01% in respect of KPI 01 to KPI 04; or
 - (ii) 0.1% in respect of KPI 05 to KPI 07; and
- C is the applicable service charges which are calculated as the aggregate of the Fixed Service Charges + Volume Based Charges for the Service Period.

KPI 08 - Service Availability: DMMP

3.6 The Service Credit due in respect of KPI 08 (Service Availability: DMMP) in each Service Period shall be calculated in accordance with the following formula:

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

$$SC = A \times B \times C$$

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 (which is 1 Service Point for each 0.01% below the Target Performance Level); and
- B** is 0.01%; and
- C** is the applicable service charges which are calculated as the aggregate of the Fixed Service Charges + Volume Based Charges for the Service Period.

Service Availability KPIs 09 and 10

- 3.7 The Service Credit due in respect of KPI 09 (Service Availability: Fixed LAN Services) and KPI 10 (Service Availability: WLAN Services) 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 (which is 1 Service Point for each 0.01% below the Target Performance Level for that Authority Site); and
- B** is the applicable Service Credit Point Value, calculated for each Authority Site in accordance with Paragraph 3.8 below.

Service Credit Point Value

- 3.8 The Service Credit Point Value for KPIs 09 and 10 are calculated for each Authority Site in accordance with the following formula:

$$\text{Service Credit Point Value} = (A \times B) / C$$

where:

- A** is the applicable Site Charge Value for the Service Period calculated in accordance with Paragraph 3.9 below; and
- B** is the applicable "At Risk Percentage" being either
- (i) 80% for a Gold Site; or
 - (ii) 65% for a Silver Site; or

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

(iii) 50% for a Bronze Site; and

C is the applicable number of "Service Credit Increments" calculated in accordance with Paragraph 3.10 below.

Site Charge Value

3.9 For the sole purpose of calculating the Service Credit Point Value for each Authority Site, the following formula shall be used:

$$\text{Site Charge Value} = \left(\frac{A}{B} \right) + C$$

where:

- A is the total Fixed Service Charges for the Service Period; and
- B is the total number of Authority Sites for the Service Period; and
- C is the apportionment of Volume Based Service Charges that are applicable to the relevant Authority Site for the Service Period (calculated by reference to the number of Devices and Device Type at the relevant Authority Site).

Service Credit Increments

3.10 The Service Credit Increments for KPIs 09 and 10 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 Service Availability Target Performance Level percentage; and
- B is the applicable Service Availability KPI Service Threshold percentage; and
- C is 0.01%.

Service Availability Performance Levels

3.11 Both the Target Performance Level percentage and KPI Service Threshold percentage for each applicable Site Availability Requirement are set out in Paragraph 11.4 of Annex 1, Part B of Schedule 3 (Performance Levels).

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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

(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 when taking into consideration 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 Not used.

6.2 Not used.

6.3 Not used.

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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, as set out in column 9 of the table in Annex F (*Allowable Assumptions*); or
- (b) on the Implementation Plan which would require adjustment under the Change Control Procedure, as identified in column 3 of the table in Annex F (*Allowable Assumptions*),

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;
- (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 'Tenderer TUPE Costs Information worksheet' as set out in Annex J of this Schedule and Schedule 8 (*Supplier Solution*) on the information provided by the Authority during the procurement process (as obtained from the Former Suppliers) as set out in Annex I (*Initial TUPE Information*) ("**the Initial TUPE Information**").

8.2 The Authority shall allow, after a Relevant Transfer from the Preceding 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

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 and the 'Tenderer TUPE Costs Information worksheet' 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.
- 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 and 'Tenderer TUPE Costs Information worksheet') have on the Charges.
- 8.8 The total value of any increase to the Charges will be capped at a maximum of 20% (twenty per cent) of the Supplier's 'Total TUPE Costs' as set out in the 'TUPE Costs Information worksheet' as set out at Annex J of this Schedule and Schedule 8 (*Supplier Solution*).

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 Authorisation Note is executed or such other date as is specified in the Change Authorisation Note.

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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 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:

Ministry of Justice

PO Box 743

Newport

Gwent

NP10 8FZ

APinvoices-MOJ-U@gov.sscl.com

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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.
- 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.

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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.
- 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.

SCHEDULE 15 (Charges and Invoicing)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- 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.

ANNEX A: MILESTONE PAYMENTS AND DELAY PAYMENTS

Milestone No.	Key Milestone	Milestone Date	Milestone Payment (£)	Milestone Retention (20%)	Delay payments
Milestone M5	First Operational Service Commencement Date (ATP Milestone)	Effective Date + 60 Working Days			A sum equal to 1/60th of 20% of the Milestone Payment for the relevant Key Milestone;
Milestone M8	Second Operational Service Commencement Date (ATP Milestone)	Effective Date + 115 Working Days			A sum equal to 1/60th of 20% of the Milestone Payment for the relevant Key Milestone;
Milestone M10	M10 - Fixed LAN and Wireless Service Transition (ATP Milestone)	Effective Date + 150 Working Days			A sum equal to 1/60th of 20% of the Milestone Payment for the relevant Key Milestone;
Milestone M11	Transition Complete (CPP Milestone)	Effective Date + 160 Working Days			A sum equal to 1/60th of 20% of the Milestone Payment for the relevant Key Milestone;

Milestone No.	Milestone	Milestone Date	Milestone Payment (£)	Milestone Retention (20%)
Milestone M1	Draft Detailed Implementation Plan	Effective Date + 40 Working Days		
Milestone M2	Contract Setup Complete	Effective Date + 40 Working Days		
Milestone M3	High Level Design	Effective Date + 40 Working Days		
Milestone M4	Service and Solution Design Complete	Effective Date + 50 Working Days		

Milestone No.	Milestone	Milestone Date	Milestone Payment (£)	Milestone Retention (20%)
Milestone M6	Soft LAN Services Support and Tooling Testing Sign Off	Effective Date + 100 Working Days	████████	████████
Milestone M7	Security Sign Off	Effective Date + 110 Working Days	████████	████████
Milestone M9	Pilot Site Acceptance Sign Off	Effective Date + 120 Working Days	████████	████████

ANNEX B: SERVICE CHARGES

1 Fixed Service Charges

Charge category	Fixed Service Charge (£) per month CY1	Fixed Service Charge (£) per month CY2	Fixed Service Charge (£) per month CY3	Fixed Service Charge (£) per month CY4	Fixed Service Charge (£) per month CY5
Hard LAN Services - Service Management Charges					
Soft LAN Services - Service Management Charges					

2 Volume Based Service Charges

2.1 Hard LAN Services – Volume Based Run and Maintain Charges, calculated as:

Total number of LAN Device Model * Monthly Unit Charge per Device Model Type from the table below:

Device Model	Vendor	Device Type	Monthly Unit Charge Per Device Type CY1	Monthly Unit Charge Per Device Type CY2	Monthly Unit Charge Per Device Type CY3	Monthly Unit Charge Per Device Type CY4	Monthly Unit Charge Per Device Type CY5
JUNIPER MIST AP32	Juniper	Access Point					
Meraki MR33-HW	Cisco	Access Point					
Meraki MR42-HW	Cisco	Access Point					
Meraki MR18-HW	Cisco	Access Point					
Meraki MR32-HW	Cisco	Access Point					
Cisco C2960	Cisco	Switch					

ANNEX B: (Service Charges)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Device Model	Vendor	Device Type	Monthly Unit Charge Per Device Type CY1	Monthly Unit Charge Per Device Type CY2	Monthly Unit Charge Per Device Type CY3	Monthly Unit Charge Per Device Type CY4	Monthly Unit Charge Per Device Type CY5
Cisco C2960 8P	Cisco	Switch					
Cisco C2960+-24PC	Cisco	Switch					
Cisco C2960+-24PC-L	Cisco	Switch					
Cisco C2960+-48PST	Cisco	Switch					
Cisco C2960C-8PC	Cisco	Switch					
Cisco C2960CX-8PC	Cisco	Switch					
Cisco C2960X 24P	Cisco	Switch					
Cisco C2960X-24PS	Cisco	Switch					
Cisco C2960X-48LPS	Cisco	Switch					
Cisco C3750X-12S	Cisco	Switch					
Cisco C3850	Cisco	Switch					
Cisco C3850-12S	Cisco	Switch					
Cisco C3850-24S	Cisco	Switch					
Cisco C3850-24T	Cisco	Switch					
Cisco C3850-48T	Cisco	Switch					
Cisco C9200-24P-4G-A	Cisco	Switch					
Cisco C9200-24P-4G-E	Cisco	Switch					
Cisco C9200-24T-E	Cisco	Switch					
Cisco C9200L 48-port 4x10G	Cisco	Switch					
Cisco C9200L 48-port PoE+ 4X10G	Cisco	Switch					
Cisco C9200L-24P-4G-A PoE+	Cisco	Switch					
Cisco C9200L-24P-4G-E	Cisco	Switch					
Cisco C9200L-24P-4G-E PoE+	Cisco	Switch					
Cisco C9200L-48P-4G-A PoE+	Cisco	Switch					
Cisco C9200L-48P-4G-E	Cisco	Switch					

ANNEX B: (Service Charges)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Device Model	Vendor	Device Type	Monthly Unit Charge Per Device Type CY1	Monthly Unit Charge Per Device Type CY2	Monthly Unit Charge Per Device Type CY3	Monthly Unit Charge Per Device Type CY4	Monthly Unit Charge Per Device Type CY5
Cisco C9200L-48P-4G-E PoE+	Cisco	Switch					
Cisco C9300 24P	Cisco	Switch					
Cisco C9300 24P-A	Cisco	Switch					
Cisco C9300 24T-E	Cisco	Switch					
Cisco C9300-24P	Cisco	Switch					
Cisco C9300-24S-A	Cisco	Switch					
Cisco C9300-24T-A	Cisco	Switch					
Cisco C9300-24T-E	Cisco	Switch					
Cisco CC9300-24T-E	Cisco	Switch					
Cisco NM-16ESW-PWR-1GI	Cisco	Switch					
Cisco WS-C2960-24TC-L	Cisco	Switch					
CISCO WS-C2960CX-8TC-L	Cisco	Switch					
HP 2530-8 PoE+	HPE / Aruba	Switch					
HP 2610-24	HPE / Aruba	Switch					
HP 2610-24 PoE	HPE / Aruba	Switch					
HP 2610-24-PWR	HPE / Aruba	Switch					
HP 2610-48-PWR	HPE / Aruba	Switch					
HP 2620-24	HPE / Aruba	Switch					
HP 2620-24 PoE+	HPE / Aruba	Switch					

ANNEX B: (Service Charges)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Device Model	Vendor	Device Type	Monthly Unit Charge Per Device Type CY1	Monthly Unit Charge Per Device Type CY2	Monthly Unit Charge Per Device Type CY3	Monthly Unit Charge Per Device Type CY4	Monthly Unit Charge Per Device Type CY5
HP 2620-48	HPE / Aruba	Switch	████	████	████	████	████
HP 2620-48 PoE+	HPE / Aruba	Switch	████	████	████	████	████
HP 2920-24G	HPE / Aruba	Switch	████	████	████	████	████
HP 2920-24G-PoE+	HPE / Aruba	Switch	████	████	████	████	████
HP 2920-48G-PoE+	HPE / Aruba	Switch	████	████	████	████	████
HP 2930F 24G POE+	HPE / Aruba	Switch	████	████	████	████	████
HP 2930F 48G POE+	HPE / Aruba	Switch	████	████	████	████	████
HP 2930F-24G-POE+	HPE / Aruba	Switch	████	████	████	████	████
HP 3810M 16SFP	HPE / Aruba	Switch	████	████	████	████	████
HP 3810M 16SFP+ 2-slot	HPE / Aruba	Switch	████	████	████	████	████
HP 5406R z12	HPE / Aruba	Switch	████	████	████	████	████
HP 5510-24G-4SPF	HPE / Aruba	Switch	████	████	████	████	████
HP 5900AF-48XG-4QSFP+	HPE / Aruba	Switch	████	████	████	████	████
HP E2620-24	HPE / Aruba	Switch	████	████	████	████	████

ANNEX B: (Service Charges)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Device Model	Vendor	Device Type	Monthly Unit Charge Per Device Type CY1	Monthly Unit Charge Per Device Type CY2	Monthly Unit Charge Per Device Type CY3	Monthly Unit Charge Per Device Type CY4	Monthly Unit Charge Per Device Type CY5
HP E2620-24 PoE+	HPE / Aruba	Switch	████	████	████	████	████
HP E2620-48	HPE / Aruba	Switch	████	████	████	████	████
HP E2620-48 PoE+	HPE / Aruba	Switch	████	████	████	████	████
HP E5412 zl	HPE / Aruba	Switch	████	████	████	████	████
HP ProCurve 3500YL-24G	HPE / Aruba	Switch	████	████	████	████	████
HP ProCurve 5400zl	HPE / Aruba	Switch	████	████	████	████	████
HPE 3800-24SFP-2SFP+	HPE / Aruba	Switch	████	████	████	████	████
Juniper EX2300-12P	Juniper	Switch	████	████	████	████	████
Juniper EX2300-24P	Juniper	Switch	████	████	████	████	████
Juniper EX2300-48P	Juniper	Switch	████	████	████	████	████
Juniper EX2300-C-12P	Juniper	Switch	████	████	████	████	████
Juniper SRX-MP-1SFP-GE 1-Port SFP GE	Cisco	Switch	████	████	████	████	████
Meraki MS120-24P-HW	Cisco	Switch	████	████	████	████	████
Meraki MS120-48FP-HW	Cisco	Switch	████	████	████	████	████
Meraki MS120-8LP-HW	Cisco	Switch	████	████	████	████	████
Meraki MS220-24P-HW	Cisco	Switch	████	████	████	████	████
Meraki MS220-8P-HW	Cisco	Switch	████	████	████	████	████
Meraki MS225-24P-HW	Cisco	Switch	████	████	████	████	████
Meraki MS410-16-HW	Cisco	Switch	████	████	████	████	████

ANNEX B: (Service Charges)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Device Model	Vendor	Device Type	Monthly Unit Charge Per Device Type CY1	Monthly Unit Charge Per Device Type CY2	Monthly Unit Charge Per Device Type CY3	Monthly Unit Charge Per Device Type CY4	Monthly Unit Charge Per Device Type CY5
Cisco SNS-3655	Cisco	Switch					
Aruba CP-HW-25K	HPE / Aruba	Switch					

2.2 Soft LAN Services – Volume Based Run and Maintain Charges, calculated as:

Total number of LAN Switches * Charge (£) per Soft LAN Switches per month plus Total number of LAN Access points * Charge (£) per Soft LAN Access points per month

LAN Device Category	Charge (£) per Device per month CY1	Charge (£) per Device per month CY2	Charge (£) per Device per month CY3	Charge (£) per Device per month CY4	Charge (£) per Device per month CY5
Soft LAN Switches					
Soft LAN Access points					

3 Catalogue Item Charges**3.1 Soft IMACD Charges**

Charge category	Number of SOFT IMACDs included in Soft LAN Service Management Charges per month	Charge (£) per month per additional Soft IMACD above threshold
Soft IMACDs		

3.2 Asset only catalogue requests

ANNEX B: (Service Charges)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Reference	Description	Lead Time	Charge (£) 1 – 10 per device	Charge (£) 11 – 50 per devices	Charge (£) 51 – 150 per device	Charge (£) 150 + per device
LAN-HW-01	8 Port Access Switch	3 Working Days				
LAN-HW-02	12 Port Access Switch	3 Working Days				
LAN-HW-03	24 Port Access Switch	3 Working Days				
LAN-HW-04	24 Port Access Switch (PoE)	3 Working Days				
LAN-HW-05	24 Port Core/Distribution Switch (configurable 10G Ports)	3 Working Days				
LAN-HW-06	48 Port Access Switch	3 Working Days				
LAN-HW-07	48 Port Access Switch (PoE)	3 Working Days				
LAN-HW-08	48 Port Core/Distribution Switch (configurable 10G Ports)	3 Working Days				
LAN-HW-09	Wireless Access Point	3 Working Days				

3.3 Hard IMACD Requests

Reference	Description	Maximum Lead Time Target (Working Days)	Unit	Lead Time(s)	One-off Charge (£s) 1st Instance	One-off Charge (£s) Subsequent Instances
LAN-HR-01	Physical survey of the Authority's Site where a wireless network is currently located or will be located in the future. These surveys must produce and provide: - Floor diagrams showing where Wireless Access Points are advised to be installed;	3	Per Instance (at the same site, on the same day)	3		

ANNEX B: (Service Charges)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Reference	Description	Maximum Lead Time Target (Working Days)	Unit	Lead Time(s)	One-off Charge (£s) 1st Instance	One-off Charge (£s) Subsequent Instances
	- Bill of Materials and any installation and cabling works required; - Heat maps; and - Wireless specifications.					
LAN-HR-02	Physical survey of the Authority's Local ICT Room/Cabinets to assess their suitability prior to the installation of new LAN devices. These surveys must take into account but not be limited to: - Power; - Cooling; - Racking; and - Cabling.	3	Per Instance (at the same site, on the same day)	3		
LAN-HR-03	Physical survey of the Authority's Local ICT Room/Cabinets to assess their suitability prior to the installation of new LAN devices. These surveys must take into account but not be limited to: - Power; - Cooling; - Racking; and - Cabling.	10	Per Instance (at the same site, on the same day)	10		
LAN-HR-04	Labour associated with the physical deployment of a switch at the Authority's Site, including all associated configuration and testing required for the switch to be integrated into the Service	10	Per Instance (at the same site, on the same day)	10		
LAN-HR-05	Labour associated with the physical deployment of a Wireless Access Point at the Authority's Site, including all associated configuration and testing required for the switch to be integrated into the Service	5	Per Instance (at the same site, on the same day)	5		
LAN-HR-06	Decommission and Secure Disposal of a switch (aligned to the Authority's Secure Disposal of IT Equipment standards)	10	Per Instance (at the same	10		

ANNEX B: (Service Charges)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Reference	Description	Maximum Lead Time Target (Working Days)	Unit	Lead Time(s)	One-off Charge (£s) 1st Instance	One-off Charge (£s) Subsequent Instances
			site, on the same day)			
LAN-HR-07	Restaging and storage of a switch to be retained for re-use elsewhere within the Authority's Estate	10	Per Instance (at the same site, on the same day)	10		
LAN-HR-08	Decommission and Secure Disposal of a Wireless Access Point (aligned to the Authority's Secure Disposal of IT Equipment standards)	10	Per Instance (at the same site, on the same day)	10		
LAN-HR-09	Restaging and storage of a Wireless Access Point to be retained for re-use elsewhere within the Authority's Estate	10	Per Instance (at the same site, on the same day)	10		
LAN-HR-10	Hard IMACD for Cabling Labour Day Rate (Installation/Patching)	1	Per Instance (at the same site, on the same day)			
LAN-HR-11	Hard IMACD for Cabling Call Out - In Hours Rate (inc, first hour on site)	1	Per Instance (at the same site, on the same day)			
LAN-HR-12	Hard IMACD for Cabling Call Out - In Hours Rate per Additional Hour	1	Per Instance (at the same site, on the same day)			
LAN-HR-13	Hard IMACD for Cabling Call Out - Out of Hours Rate (inc first hour on site)	1	Per Instance (at the same			

ANNEX B: (Service Charges)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Reference	Description	Maximum Lead Time Target (Working Days)	Unit	Lead Time(s)	One-off Charge (£s) 1st Instance	One-off Charge (£s) Subsequent Instances
			site, on the same day)			
LAN-HR-14	Hard IMACD for Cabling Call Out – Out of Hours per Additional Hour	1	Per Instance (at the same site, on the same day)			

ANNEX C: RATE CARD

Code	Role/Job Title	Daily Rate (£) 1 - 60 Days	Utilisation Discount			
			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					

ANNEX D: (Pro-Forma Certificate of Costs)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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]

Contract reference: con_24092

Contract for the provision of LAN Services

ANNEX E: RISK REGISTER

[illegible]

ANNEX F: (Allowable Assumptions)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**ANNEX F: ALLOWABLE ASSUMPTIONS**

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6	Column 7	Column 8	Column 9	Column 10	Column 11
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)
1	As requested, pricing for Hard LAN is based on a 5 year term. As such, all Third Party Contracts and Sub-contracts are based on this length of term. In the event the Contract is	None		Contract Breakage Costs as set out in Schedule 16 (Payments on Termination)	As per the Financial Model		If the Authority does not invoke the First Extension Period and Second Extension Period	At end of Initial Term or First Extension Period	Maximum of 2 years (First Extension Period and Second Extension Period)	The expiry of the Initial Term or the First Extension Period

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

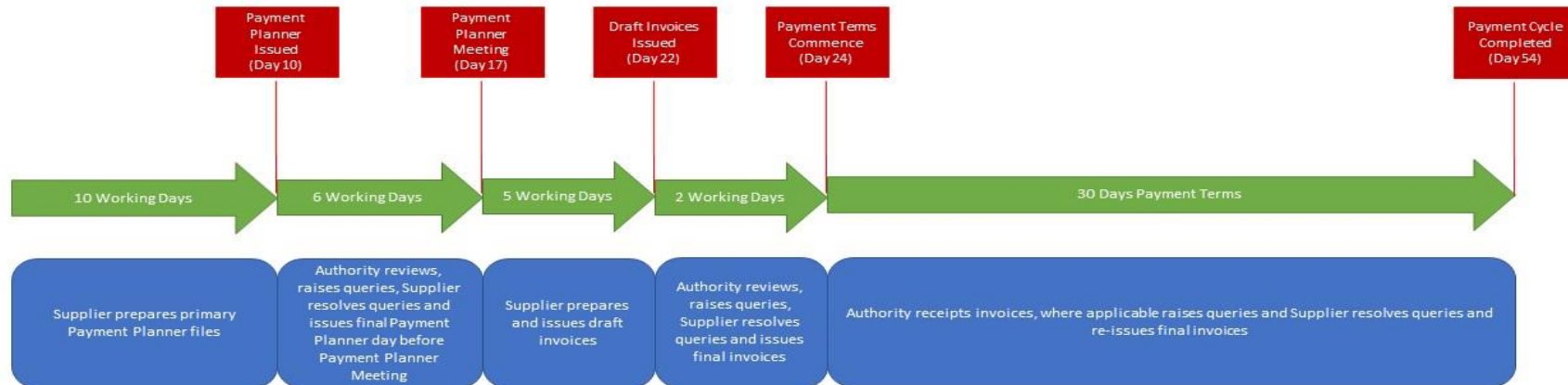
[illegible]

ANNEX G: PAYMENT PLANNER

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 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 of Part E (*Invoicing and Payment Terms*) of this Schedule 15, Paragraph 2 shall take precedence.

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 Un-invoiced Charges Report)

Payment Planner and Invoicing must always agree

ANNEX H: (Illustration of Service Points Accrual and Service Credits)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

ANNEX H: ILLUSTRATION OF SERVICE POINTS ACCRUAL AND SERVICE CREDITS

This Annex H sets out example Service Credits calculations for Service Availability KPIs (KPI-09 and KPI-10) to illustrate how the provisions of paragraphs 3.7 to 3.11 of Part C (Adjustments to the Charges and Risk Register) will be applied.

For these purposes we have based the example on Authority Sites with fixed LAN services only and have made the following assumptions:

- the total Fixed Service Charges for the relevant Service Period is £1.5m;
- the total number of Authority Sites for the Service Period is 1000 sites;
- each Authority Site has the following Fixed LAN Switches :
 - a. 20 Cisco C2960 8P
 - b. 10 Cisco C2960 Switches
- Hard LAN Services – Volume Based Run and Maintain Charge is £25 per service period per device
- Soft LAN Services – Volume Based Run and Maintain Charge is £25 per service period per device

The **Site Charge Value** (calculated in accordance with Part C paragraph 3.9) is therefore:

(Fixed Service charge /Number of Authority Site) plus

(Number of Cisco Fixed LAN Devices * Hard LAN Services – Volume Based Run and Maintain Charge) plus

(Number of Cisco devices * Soft LAN Services – Volume Based Run and Maintain Charge)

(£1.5m)/1000 plus (30 * £ 25) plus (30 * £25) = £ 3000

ANNEX H: (Illustration of Service Points Accrual and Service Credits)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

The relevant **Target Performance Level** (paragraph 3.11) per site, **KPI Service Threshold** (paragraph 3.11) per site, **Service Credit Increments** (paragraph 3.10) and applicable **At Risk Percentage** (paragraph 3.8) are as follows:

Site Classification	Service Availability Target Performance Level	Service Availability KPI Service Threshold	Service Credit Increments	Site Charge At Risk Amount (%)	Service Credit Increment
Gold	99.99%	98.99%	100	80%	0.01%
Silver	99.95%	97.99%	196	65%	
Bronze	99.90%	97.99%	191	50%	

The **Service Credit Increments** are calculated according to paragraph 3.10 as follows:

$$\text{Service Credit Increments} = \frac{A - B}{C}$$

where:

A is the applicable Service Availability Target Performance Level percentage; and

B is the applicable Service Availability KPI Service Threshold percentage; and

C is 0.01%.

The **Service Points** that will accrue for a failure to achieve the relevant Service Availability Target Performance Level percentage are 1 Service Point for each 0.01% below the Target Performance Level for that Authority Site. For example, in relation to the Gold Site in the illustrative table below, 29 Service Points will accrue if the Achieved Availability in a Service Period is 99.7%.

ANNEX H: (Illustration of Service Points Accrual and Service Credits)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

The table below illustrates how different achieved availability performance across different Authority Sites will result in differing values of Service Points. It also illustrates how the Service Credit Point Value is calculated according to paragraph 3.8 and therefore the value of Service Credits due in that Service Period.

Levels	Site Classification	Availability Target	Site Monthly Service Charges (£)	Site Charge At Risk Amount (%)	Site Charge At Risk Amount (£)	Service Credit Point Value (£)	Achieved Availability	Service Credit Points	Service Credit Due (£)
Target	Gold	99.99%	£3,000.00	80.00%	£2,400.00	£24.00	99.99%	0	£0.00
Minor	Gold	99.99%	£3,000.00	80.00%	£2,400.00	£24.00	99.70%	29	£696.00
Serious	Gold	99.99%	£3,000.00	80.00%	£2,400.00	£24.00	99.50%	49	£1,176.00
Severe	Gold	99.99%	£3,000.00	80.00%	£2,400.00	£24.00	99.00%	99	£2,376.00
Threshold	Gold	99.99%	£3,000.00	80.00%	£2,400.00	£24.00	98.99%	100	£2,400.00
Target	Silver	99.95%	£3,000.00	65.00%	£1,950.00	£9.95	99.95%	0	£0.00
Minor	Silver	99.95%	£3,000.00	65.00%	£1,950.00	£9.95	99.50%	45	£447.70
Serious	Silver	99.95%	£3,000.00	65.00%	£1,950.00	£9.95	99.00%	95	£945.15
Severe	Silver	99.95%	£3,000.00	65.00%	£1,950.00	£9.95	98.00%	195	£1,940.05
Threshold	Silver	99.95%	£3,000.00	65.00%	£1,950.00	£9.95	97.99%	196	£1,950.00
Target	Bronze	99.90%	£3,000.00	50.00%	£1,500.00	£7.85	99.90%	0	£0.00
Minor	Bronze	99.90%	£3,000.00	50.00%	£1,500.00	£7.85	99.50%	40	£314.14
Serious	Bronze	99.90%	£3,000.00	50.00%	£1,500.00	£7.85	99.00%	90	£706.81
Severe	Bronze	99.90%	£3,000.00	50.00%	£1,500.00	£7.85	98.00%	190	£1,492.15
Threshold	Bronze	99.90%	£3,000.00	50.00%	£1,500.00	£7.85	97.99%	191	£1,500.00

ANNEX I: (Initial TUPE Information)
Confidential
Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

ANNEX I – INTIAL TUPE INFORMATION

ANNEX I: (Initial TUPE Information)
Confidential
Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

[COLUMNS A – R]

[COLUMNS S – AL]

ANNEX I: (Initial TUPE Information)
Confidential
Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

[COLUMNS AL – AS]

ANNEX J: (Tenderer TUPE Costs Information Worksheet)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

ANNEX J – TENDERER TUPE COSTS INFORMATION WORKSHEET

SCHEDULE 16 (Payments on Termination)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 16
PAYMENTS ON TERMINATION

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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (a) the sum of the Unrecovered Costs and the Unrecovered Profit; and
- (b) the amount specified in Paragraph 4

“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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 32.4(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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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.

6.4 For the avoidance of doubt, where the Authority terminates the Soft LAN Services in whole or in part pursuant to Clause 31.1A (*Termination by the Authority of the Soft LAN Services*) no Compensation Payment shall be payable by the Authority.

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 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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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.

ANNEX 1: (Maximum Payments on Termination)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**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:

For the purposes of calculating the Maximum Compensation Payment below:

D = the number of days in the Shortfall Period

M = the number of complete months that have elapsed in the Contract Year

Termination Date	Maximum Unrecovered Payment	Maximum Breakage Costs Payment	Maximum Compensation Payment	
Anytime in the first Contract Year			For Soft LAN Services and any related associated services	For Hard LAN Services and any related associated services
			Where termination occurs in first 2 months of the first Contract Year: $\text{[Redacted]} \times D$ Where termination occurs in last 10 months of the first Contract Year: $\text{[Redacted]} \times D \times (1.08 - (0.04 \times M))$	$\text{[Redacted]} \times D$
Anytime in the second Contract Year			$\text{[Redacted]} \times D \times (0.6 - (0.05 \times M))$	80% of $\text{[Redacted]} \times D$
Anytime in Contract Years 3			No Compensation Payment payable	60% of $\text{[Redacted]} \times D$
Anytime during the optional Extension Period			No Compensation Payment payable	No Compensation Payment payable

SCHEDULE 17 (Benchmarking)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 17
BENCHMARKING

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

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 only be entitled to carry out a Benchmark Review of any Services during the third year of this Contract (i.e. during the 12 month period commencing on the second anniversary of the Effective 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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 are

SCHEDULE 17 (Benchmarking)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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

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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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.

Contract reference: con_24092

Contract for the provision of LAN Services

ANNEX 1: APPROVED BENCHMARKERS

Organisations Name	Address
[REDACTED]	[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 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 LAN 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

ANNEX 2: (Confidentiality Agreement)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

confidential which comes (or has come) to the Benchmarkers' attention or into the Benchmarkers' 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 Benchmarkers 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 Benchmarkers without obligation of confidentiality prior to its disclosure by the Supplier;
 - (f) the Benchmarkers obtained on a non-confidential basis from a third party who is not, to the Benchmarkers' knowledge or belief, bound by a confidentiality agreement with the Supplier or otherwise prohibited from disclosing the information to the Benchmarkers;
 - (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.

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

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) to the Contract.
- 3.3 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.
- 3.4 Before making a disclosure pursuant to Clause 3.3, 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).
- 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 Benchmarker shall be sent to:

ANNEX 2: (Confidentiality Agreement)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

[Name of Organisation]

[Address]

Attention: []

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 Benchmark]

Signature: _____

Date:

Name:

Position:

SCHEDULE 18 (Financial Distress)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 18
FINANCIAL DISTRESS

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 **Error! Reference source not found.** of this Schedule;

“Board Confirmation” means written confirmation from the Supplier’s 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, the Guarantor and the Monitored Suppliers;

“Financial Indicators” in respect of the Supplier, Key Sub-contractors and the Guarantor, 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;

“Monitored Suppliers” means those entities specified at Paragraph **Error! Reference source not found.** of this Schedule;

“Rating Agencies” the rating agencies listed in Annex 1 of this Schedule;

“Supplier’s Board” means the Supplier’s board of directors.

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, Guarantor and Key Sub-contractors satisfies the Financial Target Thresholds.
- 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) 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
 - (c) 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 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;
- (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 performance and delivery of the Services in accordance with this Contract; and
- (j) 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.

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.

SCHEDULE 18 (Financial Distress)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- 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, the Guarantor 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 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, Key Sub-contractors and/or the Guarantor 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:

SCHEDULE 18 (Financial Distress)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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 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:

SCHEDULE 18 (Financial Distress)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (a) obtaining in advance written authority from Key Sub-contractors, the Guarantor 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, the Guarantor 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:

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>>1.50 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>
2 Operating Margin	<i>Operating Margin = Operating Profit / Revenue</i>	<i>>5.00%</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>

SCHEDULE 18 (Financial Distress)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

3 Net Debt to EBITDA Ratio	<i>Net Debt to EBITDA ratio = Net Debt / EBITDA</i>	<i>< 3.50 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 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>< 5.00 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 the Net Debt and Net Pension Deficit at, the relevant accounting reference date</i>
5 Net Interest Paid Cover	<i>Net Interest Paid Cover = Earnings Before Interest and Tax / Net Interest Paid</i>	<i>> 3.00 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>
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>

SCHEDULE 18 (Financial Distress)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

8 Group Exposure Ratio	<i>Group Exposure / Gross Assets</i>	<i>< 50.00%</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 At the Effective Date there are no Monitored Suppliers, but the Authority reserves the right to regard a supplier as a Monitored Supplier as reasonably determined by the Authority, at which point the relevant category of Applicable Financial Indicators, as reasonably determined by the Authority will be applied to them.

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)
Entity e.g. Group Member, Sub-contractor, Relevant Parent Company etc. to be added in accordance with paragraph 5.2	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

A new row is to be inserted in the table above in relation to each Monitored Supplier.

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(c);

SCHEDULE 18 (Financial Distress)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (b) the Supplier fails to comply with any part of Paragraph 4.3;
- (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 Supplier's 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

SCHEDULE 18 (Financial Distress)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Effective Date if earlier than the timescale for submission set out in Paragraph 8.1 of this Schedule.

- 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.

ANNEX 1: (Rating Agencies and Their Standard Rating System)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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

ANNEX 2: CREDIT RATINGS AND CREDIT RATING THRESHOLDS

ANNEX 3: (Calculation Methodology for Financial Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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	<i>"Net Debt" = Bank overdrafts + Loans and borrowings + Finance leases + Deferred consideration payable – Cash and cash equivalents</i>

ANNEX 3: (Calculation Methodology for Financial Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

Net Debt to EBITDA Ratio	<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>

ANNEX 3: (Calculation Methodology for Financial Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

	<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><i>Net Debt</i></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><i>Net Pension Deficit</i></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><i>EBITDA</i></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 (unless ‘Net Debt + Net Pension Deficit’ is also negative, in

ANNEX 3: (Calculation Methodology for Financial Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

	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

ANNEX 3: (Calculation Methodology for Financial Indicators)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

	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

ANNEX 4: (Board Confirmation)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 19

FINANCIAL REPORTS AND AUDIT RIGHTS

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,

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
- (b) 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

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- (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.

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:

- (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

SCHEDULE 19 (Financial Reports and Audit Rights)

Security Classification (Official)

Confidential

Contract for the provision of LAN Services

Contract reference: con_24092

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 Changes to be agreed by the Parties pursuant to the report shall be subject to the Change Control Procedure.

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;
 - (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.

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.

- 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.

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, the Guarantor 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;

- (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;

- (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 LAN Services

Contract reference: con_24092

- (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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 20
ANTICIPATED SAVINGS

SCHEDULE 20 (Anticipated Savings)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Schedule 20 (*Anticipated Savings*)

[DN – 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

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 2 - REPRESENTATION AND STRUCTURE OF BOARDS and any replacements from time to time agreed by the Parties in accordance with Paragraph 6.3;
“Boards”	the Joint Strategic Partnership Board, Supplier Governance Board, All Supplier Forum, Exit and Transition Board, Service Board, Commercial Board, Project Portfolio Board, Finance Review Meetings, Project Meetings, Risk Management Board, Commercial Review Meetings, Enterprise Architecture Board and Supplier Performance Review Board and “Board” shall mean any of them;
“Project Managers”	the individuals appointed as such by the Authority and the Supplier for individual projects;;

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.

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 set out at Annex 1 (Governance Principles) and Annex 2 (Representation and Structure of Boards).

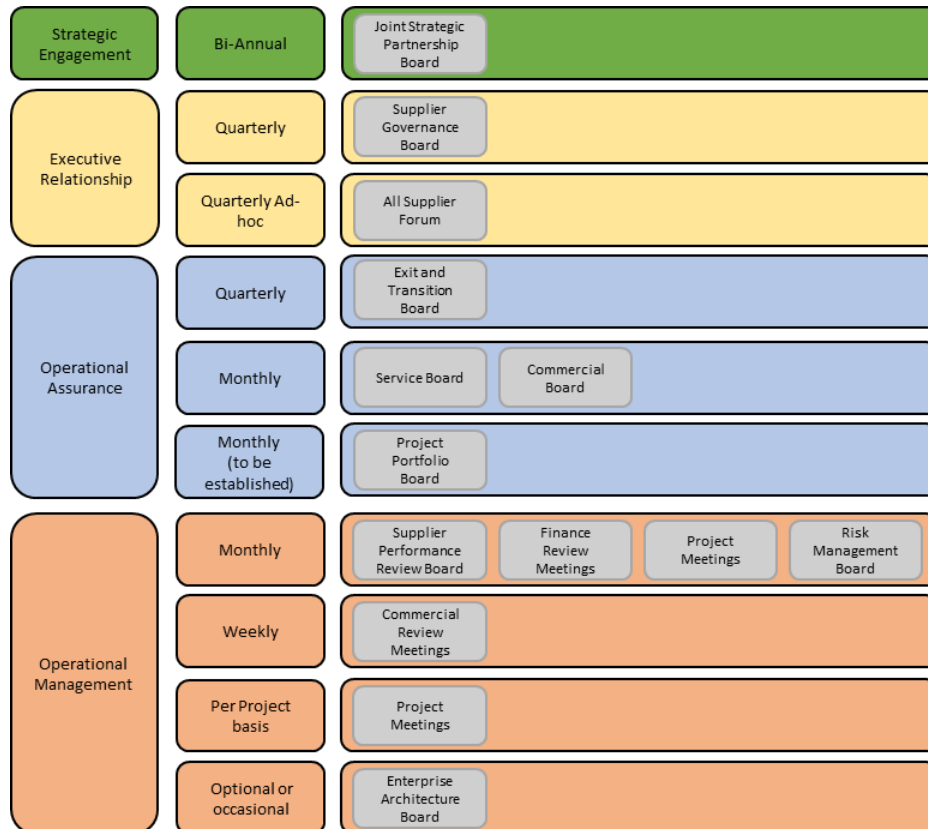


Figure 1 – Governance Framework

4 MANAGEMENT OF THE SERVICES

- 4.1 The Supplier and the Authority shall each appoint a Project 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.
- 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 board 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 ICT 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.

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, 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.

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. 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.

SCHEDULE 21 (Governance)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 6.5 A chairperson shall be appointed by the Authority for each Board as identified in ANNEX 2 - REPRESENTATION AND STRUCTURE OF BOARDS. 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.
- 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 In addition to the Boards outlined in this Schedule, an annual review meeting shall be held throughout the Term on a date to be agreed between the Parties.

SCHEDULE 21 (Governance)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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.

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.

- 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 but not limited to, the delivery of the Operational Services to the Authority in accordance with the Performance Indicators.
- 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 the Supplier's 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 the formal Governance 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, but not be limited to:
 - (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;
 - (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, but not be limited to:
 - (a) Frequency;
 - (b) Type;
 - (c) Chair;
 - (d) Input to;
 - (e) Team 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, which shall consist of, but shall not be limited to the following:
- (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, but not limited to:
 - (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.

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 3.6(d)). The Supplier shall support the Authority in delivering the services as described in paragraph 3.6(d) through, including but not limited to:

- (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.

ANNEX 2 - REPRESENTATION AND STRUCTURE OF BOARDS**Joint Strategic Partnership Board – Steering Level**

Responsibilities and Functions of the Joint Strategic Partnership Board	Act as forward-looking forum to enable the Authority to deliver its vision and to review spending challenges 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. Review the overall effectiveness of the Services in meeting the needs of the Authority's business. 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. Resolve relationship issues and issues relating to this Contract which are escalated to the Joint Strategic Partnership Board. Formal escalation body from the Supplier Governance Board. Making escalations to the Authority executive team.
Authority Members of Joint Strategic Partnership Board	Senior Business Owner Chairperson Senior Prison Service Representative

ANNEX 2: (Representation and Structure of Boards)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	Commercial Manager Senior Architect Cross Government Representative (as required)
Supplier Members of Joint Strategic Partnership Board	Account Director Senior Contract Specialist Senior Commercial Specialist Technical Design Authority
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	Bi-annually
Location of Joint Strategic Partnership Board meetings	102 Petty France or 10 South Colonnade

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. Note that this forum's function relates to relationship management rather than contract management.
Authority Members of All Supplier Forum	Senior Business Owner Chairperson Service Owner Senior Architect

ANNEX 2: (Representation and Structure of Boards)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	Commercial Manager
Supplier Members of All Supplier Forum	Account Director Service Manager Senior Contract Specialist Senior Commerical Specialist Technical Design Authority
Start Date for All Supplier Forum	Post Effective Date to align with the Authority governance framework
Frequency of All Supplier Forum	Quarterly Ad-hoc
Location of All Supplier Forum	102 Petty France or 10 South Colonnade

Supplier Governance Board – Executive Level

Responsibilities and Functions of the Executive Partnership 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.

ANNEX 2: (Representation and Structure of Boards)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

	Serve as an executive escalation forum to resolve 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	Senior Business Owner Chairperson Commercial Manager Digital Finance Manager Finance Business Partner Risk Manager Operations Manager Project Management (as required) Contract Management Team
Supplier Members of Supplier Governance Board	Account Director Senior Contract Specialist Senior Commercial Specialist Service Manager Programme Manager (as required) Project Manager (as required)
Start Date for Supplier Governance Board meetings	Post first Operational Service Commencement Date
Frequency of Supplier Governance Board meetings	Quarterly
Location of Supplier Governance Board meetings	102 Petty France or 10 South Colonnade

Exit and Transition Board – Operational Assurance Level

Responsibilities and Functions of the Exit and Transition Board	Develop a strategy for exit and transition. Manage and review the Exit Plan. Oversee the implementation of the Exit Plan until the conclusion of all activities set out in the Exit Plan. Review the associated Registers. Review progress on the Implementation Plans and transition matters. Assess the impact of further technology refresh triggers. Manage the documentation required to support Implementation Plan(s) and/or Exit Plan(s) (for example, asset registers). Review of 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 Exit and Transition Board	Exit Manager Chairperson Service Owner Service Lead (as required) Commercial Manager Authority RepresentativeDigital Finance Manager Risk Manager Project Management
Supplier Members for Exit and Transition Board	Account Director (where required) Programme Manager Project Manager Service Manager Senior Commercial Specialist

ANNEX 2: (Representation and Structure of Boards)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

	Senior Contract Specialist
Start Date for Exit and Transition Board meetings	Post first Operational Service Commencement Date
Frequency of Exit and Transition Board meetings	No less than quarterly per Contract Year, or as required in order to effectively manage updates and Implementation and/or Exit Plan(s).
Location of Exit and Transition Board meetings	102 Petty France or 10 South Colonnade

Service Board – Operational Assurance Level

Responsibilities and Functions of the Service 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. Request and review reports from the Exit Managers on each Party's compliance with Schedule 25 (Exit Management), particularly in relation to the production and updating of the Exit Plan and the provision of any Termination Services. In the event of any termination (in whole or in part) or expiry of this Contract, manage performance by the Supplier and the Authority of their respective obligations in relation to Schedule 25 (Exit Management), acting as an escalation point for the Exit and Transition Board. Formal escalation body from the Exit and Transition Board.

ANNEX 2: (Representation and Structure of Boards)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	Review of 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 Board	Service Owner Chairperson Service Manager Commercial Manager Authority Representative Digital Finance Manager (as required) Risk Manager (as required) Project Management (as required)
Supplier Members for Service Board	Service Manager Senior Commercial Specialist (as required) Senior Contract Specialist Contract Specialist Account Director (as required) Programme Manager (as required) Project Manager (as required)
Start Date for Service Board meetings	Post Effective Date to align with the Authority governance framework
Frequency of Service Board meetings	Monthly or as required by the Authority from time to time.
Location of Service Board meetings	102 Petty France or 10 South Colonnade

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). 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.

ANNEX 2: (Representation and Structure of Boards)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

	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	Commercial Manager Chairperson Authority Representative Digital Finance Manager
Supplier Members for Commercial Board	Account Director (as required) Senior Commercial Specialist Senior Contract Specialist Contract Specialist
Start Date for Commercial Board meetings	Post first Operational Service Commencement Date
Frequency of Commercial Board meetings	Monthly or as required by the Authority from time to time.
Location of Commercial Board meetings	102 Petty France or 10 South Colonnade

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.

ANNEX 2: (Representation and Structure of Boards)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

	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	Service Owner Chairperson Service Lead (as necessary) Commercial Manager Risk Manager
Supplier Members for Project Portfolio Board	[Equivalent Supplier Representatives] Account Director (as required) Service Manager Senior Commercial Specialist Senior Contract Specialist Contract Specialist
Start Date for Project Portfolio Board meetings	Post first Operational Service Commencement Date
Frequency of Project Portfolio Board meetings	Monthly (to be established).
Location of Project Portfolio Board meetings	102 Petty France or 10 South Colonnade

Supplier Performance Review Board – Operational Management Level

Responsibilities and Functions of the Supplier Performance Review Board	Review the Supplier's performance including any Balanced Scored. Service Performance: a) Review the Supplier's performance against Performance 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. 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 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

ANNEX 2: (Representation and Structure of Boards)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	agenda item. Share output of risk review with cascading Boards/forums.
Authority Members for Supplier Performance Review Board	Service Owner Chairperson Commercial Manager Authority Representative Digital Finance Manager Risk Manager Project Management
Supplier Members for Supplier Performance Review Board	Senior Commercial Specialist Senior Contract Specialist Programme Manager Project Manager
Start Date for Supplier Performance Review Board meetings	Post first Operational Service Commencement Date
Frequency of Supplier Performance Review Board meetings	Monthly or as required by the Authority from time to time. To be held before the monthly Service Board.
Location of Supplier Performance Review Board meetings	102 Petty France 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

ANNEX 2: (Representation and Structure of Boards)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	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. [Note: Supplier to circulate risk treatment plan 5 days in advance of each meeting.]
Authority Members for Risk Management Board	Strategic Risk Manager Chairperson Service Owner Commercial Manager Authority Representative Service Lead (as required)
Supplier Members for Risk Management Board	Account Director (as required) Senior Commercial Specialist Senior Contract Specialist Programme Manager Project Manager]
Start Date for Risk Management Board	Post first Operational Service Commencement Date
Frequency of Risk Management Board	Monthly or as required by the Authority from time to time.
Location of Risk Management Board	102 Petty France or 10 South Colonnade

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.

ANNEX 2: (Representation and Structure of Boards)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

	Review the financial reports submitted by the Supplier.
Authority Members for Finance Review Meetings	Service Owner Chairperson Service Lead (if required) Commercial Manager Authority Representative Digital Finance Manager
Supplier Members for Finance Review Meetings	Account Director (as required) Service Manager Senior Commercial Specialist Senior Contract Specialist Contract Specialist
Start Date for Finance Review Meetings	Post first Operational Service Commencement Date
Frequency of Finance Review Meetings	Monthly or as required by the Authority from time to time.
Location of Finance Review Meetings	102 Petty France or 10 South Colonnade

Project Meetings – Operational Management Level

Responsibilities and Functions of the Project Meetings	Discuss any address any open risks and that may impact the delivery of Services. 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	Project Manager Chairperson Service Lead (as required)

ANNEX 2: (Representation and Structure of Boards)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Supplier Members for Project Meetings	Account Director (as required) Project Manager Programme Manager (as required) Service Manager (as required) Senior Contract Specialist (as required) Senior Commercial Specialist (as required)
Start Date for Project Meetings	Post first Operational Service Commencement Date
Frequency of Project Meetings	Monthly and as otherwise decided on a per project basis.
Location of Project Meetings	102 Petty France 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. 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	Commercial Manager Chairperson Authority Representative Digital Finance Manager
Supplier Members for Commercial Review Meetings	Senior Commercial Specialist Senior Contract Specialist

ANNEX 2: (Representation and Structure of Boards)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

Start Date for Commercial Review Meetings	Post first Operational Service Commencement Date
Frequency of Commercial Review Meetings	Weekly or as required by the Authority from time to time.
Location of Commercial Review Meetings	102 Petty France 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. 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

ANNEX 2: (Representation and Structure of Boards)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

	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	Senior Architect Chairperson Additional MoJ IT representatives
Supplier Members for Enterprise Architecture Board	Account Director (as required) Service Manager Technical Design Authority Additional BT Technical Representatives
Start Date for Enterprise Architecture Board meetings	Post first Operational Service Commencement Date
Frequency of Enterprise Architecture Board meetings	Optional or occasional.
Location of Enterprise Architecture Board meetings	102 Petty France or 10 South Colonnade

**SCHEDULE 22 (Change Control Procedure,
Service Requests and Projects)**

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 22

**CHANGE CONTROL PROCEDURE, SERVICE
REQUESTS AND PROJECTS**

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 and Projects)**

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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.

**SCHEDULE 22 (Change Control Procedure,
Service Requests and Projects)**

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

2.6 The Supplier shall:

- (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.

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 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

**SCHEDULE 22 (Change Control Procedure,
Service Requests and Projects)**

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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:
 - (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;

**SCHEDULE 22 (Change Control Procedure,
Service Requests and Projects)**

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- (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:
- (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 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 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.

**SCHEDULE 22 (Change Control Procedure,
Service Requests and Projects)**

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 Manager, as applicable. The provisions of Clause 42 (*Notices*) shall apply to a Change Communication as if it were a notice.

ANNEX 1: (Change Request Form)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**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:		

ANNEX 2: (Change Authorisation Note)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**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: _____	

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
- 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.

- 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) 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 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 fulfilling 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 delivering 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;
 - 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 4.2, 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 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 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 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, then either;
- 7.1.1 the Supplier shall prepare two final 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; or
 - 7.1.2 the Supplier shall prepare a final copy of a Project Work Order which, using an agreed electronic signature application, it shall sign and deliver to the Authority for its signature.
 - 7.1.3 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 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 9.3 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

- 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.

ANNEX 1: (Project Work Order Template)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**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			

2 INTRODUCTION

- 2.1 This Project Work Order ("PWO") constitutes an addition to the Contract for [] entered into on [xxxx] (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.]

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			

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.

7.4.2 The service charge shall be invoiced monthly in arrears against the [Insert Reference to Standard Invoice] and recorded on the Payment Planner.

- 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

[To evidence approval by both Parties, all documents that are intended to indicate approval must be signed by the Representative of each Party]

ANNEX 1: (Project Work Order Template)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

**Signed and agreed on behalf of the
Supplier**

**Signed and agreed on behalf of the
Authority**

.....
Signature

.....
Signature

.....
Name

.....
Name

.....
Position

.....
Position

.....
Date

.....
Date

ANNEX 1: (Project Work Order Template)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**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

ANNEX 1: (Project Work Order Template)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

			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

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

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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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.

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 **[insert role]** and the Supplier's **[insert role]**.

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.

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;

- (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.

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;
- (e) the chair of the arbitral tribunal shall be British;
- (f) the arbitration proceedings shall take place in London and in the English language; and
- (g) the seat of the arbitration shall be London.

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:

SCHEDULE 23 (Dispute Resolution Procedure)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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.
- 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

SCHEDULE 23 (Dispute Resolution Procedure)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 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 reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

SCHEDULE 24

REPORTS AND RECORDS PROVISIONS

Schedule 24 (*Reports and Records Provisions*)

1 TRANSPARENCY REPORTS

- 1.1 Within three (3) months of the Effective Date the Supplier shall provide to the Authority for its approval (such approval not to be unreasonably withheld or delayed) draft transparency reports in accordance with (and identified as transparency reports in) Annex 1 (once approved, the “**Transparency Reports**”).
- 1.2 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.
- 1.3 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.
- 1.4 Any disagreement in connection with the preparation and/or approval of Transparency Reports, other than under Paragraph 1.2 above in relation to the contents of a Transparency Report, shall be treated as a Dispute.
- 1.5 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.

3 RECORDS

- 3.1 The Supplier shall retain and/or maintain all the Records (as appropriate) subject to Paragraph 4.18, ::

SCHEDULE 24 (Reports and Records Provisions)

Confidential

Security Classification (Official)

Contract for the provision of LAN Services

Contract reference: con_24092

- (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 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

SCHEDULE 24 (Reports and Records Provisions)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

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 Supplier pursuant to Paragraph 2.1 of Schedule 32 (*Intellectual Property Rights*) of this Contract. The Supplier shall grant to the Authority and the Service Recipients licences to use the Project Specific IPR in the Virtual Library pursuant to Paragraph 2.5 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:
- (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

SCHEDULE 24 (Reports and Records Provisions)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

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.

ANNEX 1: (Reports Including Transparency Reports)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**ANNEX 1: REPORTS INCLUDING TRANSPARENCY REPORTS**

TITLE	CONTENT/Definition	TRANSPARENCY REPORT (Y/N)	FREQUENCY
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	N	Within 1 Month of Effective Date
Balanced and Scorecard Report	has the meaning given in Paragraph 1.3 of Part B of Schedule 3. A report created by the Supplier to the Authority's senior responsible officer which summarises the Supplier's performance over the relevant Service Period as more particularly described in Paragraph 1.3 (the "Balanced Scorecard Report").	N	Upon request from the Authority
Performance Monitoring Report	a report to the Authority Representative which summarises the performance by the Supplier against each of the Performance Indicators as more particularly described in Paragraph 1.2, Part B of Schedule 3 (Performance Levels)	N	Each Service Period
Sustainability Reports	written reports to be completed by the Supplier containing the information outlined in Table C of Annex 1 Schedule 4 (Standards)	N	As outlined in Table C of Annex 1 Schedule 4 (Standards)
Test Report	the reports to be produced by the Supplier setting out the results of Tests in accordance with Schedule 14 (Testing Procedures)	N	As required by the Authority in accordance with Schedule 14
Benchmark Report	the report produced by the Benchmarker following the Benchmark Review as further described in Paragraph 5 of Schedule 17 (Benchmarking);	N	As required by the Authority in accordance with Schedule 17

ANNEX 1: (Reports Including Transparency Reports)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

TITLE	CONTENT/Definition	TRANSPARENCY REPORT (Y/N)	FREQUENCY
Annual Contract Report	the annual contract report to be provided by the Supplier to the Authority pursuant to Paragraph 1 of Part B of Schedule 19; (c) the Authority's internal and external auditors; (d) the Authority's statutory or regulatory auditors; (e) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; (f) HM Treasury or the Cabinet Office; (g) any party formally appointed by the Authority to carry out audit or similar review functions; and successors or assigns of any of the above	N	Within 1 Month of the end of the Contract Year to which that report relates
Contract Amendment Report	the contract amendment report to be provided by the Supplier to the Authority pursuant to Paragraph 1 of Part B of Schedule 19 (Financial Reports and Audit Rights)	N	Within 1 Month of a Material Change being agreed between the Supplier and the Authority
Final Reconciliation Report	the final reconciliation report to be provided by the Supplier to the Authority pursuant to paragraph 1 of Part B of Schedule 19 (Financial Reports and Audit Rights)	N	Within 6 Months after the end of the Term
Onerous Contract Report	means a report provided by the Supplier pursuant to paragraph 3 of Part A to Schedule 19 (Financial Reports and Audit Rights);	N	As required by the Authority in accordance with Schedule 19
Quarterly Contract Report		N	Within 1 Month of the end of each Quarter
Financial Indicator Reports	Subject to the calculation methodology set out at Schedule 18 (Financial Distress) paragraph 5 Financial Indicators	N	Reported yearly in arrears within 120 days of each Accounting Reference Date

ANNEX 1: (Reports Including Transparency Reports)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

TITLE	CONTENT/Definition	TRANSPARENCY REPORT (Y/N)	FREQUENCY
			based upon figures for the 12 Months ending on the relevant Accounting Reference Date.
Service Continuity Plan Review Report	has the meaning given in Paragraphs 7.2(a) to 7.2(c) of Schedule 26 (Service Continuity Plan and Corporate Resolution Planning)	N	Within 20 Working Days of the conclusion of each such review of the Service Continuity Plan
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 (Reports and Records Provisions)	Y	Refer to Annex 4 of this Schedule.
Financial Reports	the Contract Inception Report and the reports listed in the table in Paragraph 1.1 of Part B of Schedule 19 (Financial Reports and Audit Rights)	N	As required by the Authority in accordance with Schedule 19
Major Incident Report	the report that is produced in relation to a Major Incident and that describes the nature of the incident and recovery actions taken;	N	Following the agreed closure of a major incident and as reasonably requested to support the production of the Major Incident Report.
Post Go Live Report	a report covering activities completed post the relevant Operational Services Commencement Date and initial period of Early Life Support, which details any risks, issues or defects identified	N	Five (5) Working Days after the responsibility for the Services at an Authority Site have transferred from the Preceding Supplier to the Supplier or after an Operational Services Commencement Date.

ANNEX 1: (Reports Including Transparency Reports)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

TITLE	CONTENT/Definition	TRANSPARENCY REPORT (Y/N)	FREQUENCY
Root Cause Analysis Reports	refer to Schedule 2 Annex B (Service Management Requirements) para 6.5.3.3	N	Within 10 Working Days of Authority request.
Status Reports	detailing new Incidents, vulnerabilities, mitigations, and providing an overview of long-term rectification plans (e.g. for low priority items) as required in Paragraph 7.6 of Schedule 5 (Security Management);	N	Monthly
Transition Closure Report	the final transition Deliverable for a project and is used for senior management to assess the success of the Transition. The closure report records the final project sign off from the sponsor, assesses success, and initiates a number of activities: identify and share best practices for future transition projects;	N	At the end of the project
Payment Planner		N	Monthly in accordance with Schedule 15 (Charges and Invoicing)
IT Health Check report	As described in Paragraph 9.1 (a) of Schedule 5 (Security Management)	N	Repeat the IT Health Check not less than once every 12 months during the Term

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 and/or the Guarantor, 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 Guarantor and 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.

ANNEX 2: (Records to be kept by the Supplier)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 17 All journals and audit trail data referred to in Schedule 5 (*Security Management*).
- 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 Authority's ITSM toolset that are within the scope of the Supplier's responsibilities, including requirements 6.4.7.17, 6.5.2.4, 6.5.3.5 and 6.5.4.2 in Annex B (LAN Service Management Requirements) to Schedule 2 (Services Description).

ANNEX 3: (Records to upload to Virtual Library)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**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)
CI.5.5 (e), (f), 5.8(b), Paragraphs 2.1(a) and 2.2(a)(ii)	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.	-	Authority
CI 14.3	[Key Personnel]	Schedule 29	Effective Date	On replacement of Key Personnel	Authority
Schedule 5, Para 4.2	Core Information Management System diagram	Schedule 5, Annex 3	The date specified in the Detailed Implementation Plan	Regular review and at least annually	Authority
Sch 5, Para 13.1	Security Reports	As appropriate and agreed by the Authority	As requested by the Authority	Frequency and nature of which shall be as detailed and agreed in the Security Management Plan	Authority
Schedule 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

ANNEX 3: (Records to upload to Virtual Library)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)
Schedule 5, Para 7	Security Certification Requirements	Schedule 5,	Prior to receiving, storing or processing any Authority Data	-	-
Schedule 6, Para 4	Evidence of Insurances	Schedule 6	Effective Date	Within fifteen (15) days after policy renewal or replacement	Authority
Schedule 9	Commercially Sensitive Information	Schedule 9	Effective Date	Upon agreement by the Authority to vary the information	Authority and/or Auditor
Schedule 10	Notified Key Subcontractors	Schedule 10	Effective Date	On replacement of key subcontractor	Authority
Schedule 11, Para 1	Third Party Contracts	Schedule 11	Effective Date	On appointment of subcontract	Authority
CI 15.6 and 15.7	Notified Key Sub-Contractors	Schedule 10	Effective Date	With each approved appointment or variation	Authority
CI 15.28	Supply chain Transparency Reports	Schedule 24, Annex 4	Thirty days prior to the of the end of each financial year	Every twelve (12) months	Authority
CI 6.4	Detailed Implementation Plan	Schedule 13	Within 20 Working Days of Effective Date	Every 3 months from Effective Date	Authority
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

ANNEX 3: (Records to upload to Virtual Library)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)
Schedule 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
Schedule 14, Para 5	Test Plan	As appropriate and agreed by the Authority	20 Working Days prior to the relevant test	Upon update to the test plan	Authority
Schedule 14, Para 7	Test Specification	As appropriate and agreed by the Authority	10 Working Days prior to the relevant test	Upon update to the test specification	Authority
Schedule 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 to end for the Draft Test Report 5 days for the Final Test Report following the relevant test completion	Reissue with each retest	Authority
Schedule 15, Annex 4	Risk Register	Schedule 15, Annex 4	Effective Date	Upon agreement by the Authority to vary the by the Risk Management Board	Authority
Schedule 17, Para 4	Benchmarking Plan	Schedule 17	Upon receipt from Benchmarker	Approval of Plan	Authority and Auditor
Schedule 17, Para 5	Benchmarking report	Schedule 17	Upon receipt from Benchmarker	Any update	Authority and Auditor

ANNEX 3: (Records to upload to Virtual Library)

Confidential

Security Classification (Official)

Contract for the provision of LAN Services

Contract reference: con_24092

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)
Schedule 18, Para 2.3(b)	Financial Indicator Reports	Schedule 18, Para 2.5	As specified in Para2.3(b) of Schedule 18	As specified in Para 2.3(b) of Schedule 18	Authority
Schedule 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
Schedule 19, Part B, Para 1.1	Contract Amendment Report	Schedule 19, Part B, Para 1.2	Within 1 month of a material change being agreed	-	Authority
Schedule 19, Para 1.1	Quarterly Contract Report	Schedule 19, Part B, Para 1.2	Within 1 month of the end of each Quarter	-	Authority
Schedule 19, Part B, para 1.1	Annual Contract Report	Schedule 19, Part B, Para 1.2	Within 1 month of the end of the Contract Year to which that report relates	-	Authority
Schedule 19, Part B, para 1.1	Financial Reconciliation Report	Schedule 19, Part B, Para 1.2	Within 6 months after the end of the Term	-	Authority
Schedule 21, Para 3.3	Representation and Structure of boards	Schedule 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
Schedule 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

ANNEX 3: (Records to upload to Virtual Library)

Confidential

Security Classification (Official)

Contract for the provision of LAN Services

Contract reference: con_24092

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)
Schedule 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
Schedule 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
Schedule 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
Schedule 22, Para 4	Change Request	Schedule 22, Annex 1	Within 10 Working Days of Authority issuing the Change Request	-	Authority
Schedule 23, Para 2.1	Dispute Notice	Schedule 23 Para 2.2	No longer than 20 Working Days from an unresolved dispute arising	Any variation	Authority
Schedule 23, Para 2.4	Mediation Notice	As appropriate	When first served	Any variation	Authority
Schedule 24, Para 1	Reports and Records Provisions	Schedule 24, Annex 1	Within 3 months of the Effective Date	Frequency specified in Schedule 24, Annex 1	Authority
Schedule 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

ANNEX 3: (Records to upload to Virtual Library)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)
Schedule 25, Para 2.1(b)	Configuration Database of Technical Infrastructure and Operating Procedures	As appropriate and agreed by the Authority	Within 3 months of the Effective Date	Any variation	Authority
Schedule 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
Schedule 25, Para 5.1	Exit Plan	Schedule 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
Schedule 25, Para 6.3(e)	Provide up to date Registers during the Termination Assistance Period	As appropriate	As requested by the Authority	As appropriate	
Schedule 25, Para 6.7(b)	Authority Data (handback)	Schedule 25, Para 3 and/or as appropriate and agreed by the Authority	At the end of the Termination Assistance Period	-	Authority
Schedule 25, Annex	Termination Services	As appropriate	As specified in the Termination	As specified in the	-

ANNEX 3: (Records to upload to Virtual Library)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)
1, Para 1.1, Para 1.2 Para 1.3 & Para 1.4	supporting documentation and knowledge transfer material	and agreed by the Authority	Assistance Notice and in any event prior to the end of the Termination Assistance Period	Termination Assistance Notice or otherwise requested by the Authority	
Schedule 26 Service Continuity	Service Continuity Plan	Schedule 26, Para 2.2	Within 40 Working Days from the Effective Date	Schedule 26, Para 7.1	Authority
Schedule 26, Para 7.2	Service Continuity Plan Review Report	Schedule 26, Para 6.2	Within 20 Working Days of the conclusion of each review of the Service Continuity Plan.	-	-
Schedule 26, Part B	Corporate Resolution Planning Information	Schedule 26, Part B, Para 2.3	Schedule 26 Part B Para 2.2	Schedule 26, Para 11.8	Authority
Schedule 2, Annex B, requirement 6.3.4.4	Action tracker for Supplier actions agreed at the monthly IT Service Continuity forums	As appropriate and agreed by the Authority	At the first monthly IT Service Continuity forum	Monthly	Authority
Schedule 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
Schedule 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

ANNEX 3: (Records to upload to Virtual Library)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)
Schedule 18 Para 8	Board Confirmation	As set out at Annex 4 of Schedule 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
Schedule 28, Part E, Para 1.1	Supplier's Provisional Supplier Personnel List and, Staffing Information	As appropriate and agreed by the Authority	Schedule 28, Para 1.1(a) - (d)	At such intervals as are reasonably requested by the Authority	Authority
Schedule 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
Schedule 2, Annex B, requirement 6.4.1.8	List of Supplier Staff who are authorised by the Supplier to submit an RFC	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
Schedule 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
Schedule 28, Part E, Para 1.7	Payroll and benefits information	As appropriate and agreed	Within 5 Working Days following the	-	Authority, any Replacement Supplier and/or Replacement

ANNEX 3: (Records to upload to Virtual Library)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)
		by the Authority	Service Transfer Date		Sub-contractor
Schedule 28, Annex E1	List of Notified Sub-contractors	As appropriate and agreed by the Authority	Effective Date	Upon any change	Authority
Schedule 29	Key Personnel	Schedule 29	Effective Date	As amended from time to time	Authority
Schedule 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
Schedule 2 Annex B, requirement 6.4.4.4	Records of all Configuration Items, Assets and Authority Assets including spares, both past and present, and their current status	Service Asset and Configuration Management System	As agreed with Authority	Upon any change	Authority
Schedule 2 Annex B, requirement 6.3.2.3	Capacity Plan	As appropriate and agreed by the Authority	As agreed with Authority	As agreed with Authority	Authority and Supplier
Schedule 2 Annex B, requirement 6.5.5.9	Service Improvement Plan	As appropriate and agreed by the Authority	As agreed with Authority	As agreed with Authority	Authority and Supplier
Schedule 2 Annex B, requirement 6.5.6.6	List of Supplier Personnel who require access to the Authority's ITSM Toolset and their	As appropriate and agreed by the Authority	As agreed with Authority	Any variation	Authority

ANNEX 3: (Records to upload to Virtual Library)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

Applicable Clause/ Paragraph	Required Data	Format of Data	Initial Upload Date	Update Requirement	Access Permission and Access Event (where applicable)
	required permission level.				
Schedule 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
Schedule 2 Annex A , requirement 2.1.1.26	Device backups	As appropriate and agreed by the Authority	As agreed with Authority	As agreed with Authority	Authority and Supplier
Schedule 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

ANNEX 3: (Records to upload to Virtual Library)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

The following table defines the Knowledge Management Artefacts to be stored in the Authority's Knowledge Management System, but does not exclude additional documentation that may be reasonably added by the Parties, at a later date.

Knowledge Management Artefacts
Knowledge articles
Training material
Minimum data sets
Solution designs, architectural documentation (including high-level designs, low-level designs, Service Design Packages)
Event Management triggers, thresholds and responses
Dependency mapping, Service Component Failure Impact Analysis
Configuration documentation
Blueprints, templates and patterns
Policies, processes and procedures

ANNEX 3: (Records to upload to Virtual Library)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Knowledge Management Artefacts	
Organisational diagrams, escalation paths, contact lists	
Change models, standard change designs / definitions	
Build instructions/runbooks	
Release and deployment plans	
Test plans	
IT service continuity plans, business impact analyses and risk assessments	
Performance Monitoring Reports	
Minutes of meetings	

ANNEX 4: (Supply Chain Transparency Information Template)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**ANNEX 4: SUPPLY CHAIN TRANSPARENCY INFORMATION TEMPLATE**

	Financial Year 20[]			
	Under this Contract		Supplier as a whole	
	£	%	£	%
Estimated total contract revenue (£) to be received in this Financial Year	£[]	100%	£[]	100%
Total value of Sub-contracted revenues (£) in this Financial Year	£[]	[]	£[]	[]
Total value of Sub-contracted revenues to SMEs (£) in this Financial Year	£[]	[]	£[]	[]
Total value of Sub-contracted revenues to VCSEs (£) in this Financial Year	£[]	[]	£[]	[]

SCHEDULE 25 (Exit Management)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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;

“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(b).

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;
 - (B) ownership and status as either Exclusive Assets or Non-Exclusive Assets;

SCHEDULE 25 (Exit Management)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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;
- (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 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 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.

SCHEDULE 25 (Exit Management)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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:

- (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

SCHEDULE 25 (Exit Management)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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;
 - (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).

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;

SCHEDULE 25 (Exit Management)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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 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);
 - (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.
- 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;

SCHEDULE 25 (Exit Management)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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**");
 - (i) which, if any, of:
 - (A) the Exclusive Assets that are not Transferable Assets; and
 - (B) the Non-Exclusive Assets,

the Authority and/or the Replacement Supplier requires the continued use of; and
- (b) 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 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

SCHEDULE 25 (Exit Management)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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(b) 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 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:

SCHEDULE 25 (Exit Management)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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.

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.

11 PARTIAL TERMINATION OF SOFT LAN SERVICES]

- 11.1 If the Authority elects to partially terminate the Soft LAN Services (in whole or in part) and any associated Services that are no longer required following termination of the Soft LAN Services in accordance with Clause 31.1A (Termination by the Authority), the Authority shall provide written notification (the “**Initial Cease Notice**”) to the Supplier that it intends to terminate the Soft LAN 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 Soft LAN Services to be terminated;
 - 11.1.2 the Termination Assistance, if required and known by the Authority at this stage;

SCHEDULE 25 (Exit Management)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 11.1.3 the forecast date(s) on which the Soft LAN 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 Soft LAN 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;
 - 11.3.4 details of the impact of terminating the Soft LAN Services 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 Soft LAN Services;
 - 11.3.6 particulars of any changes which would be required to the Exit Plan in order to terminate the Soft LAN 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 Soft LAN Services;

SCHEDULE 25 (Exit Management)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 11.3.8 a detailed breakdown and such supporting evidence of the costs and resources reasonably required to successfully cease the Soft LAN Services by the forecast date(s);
 - 11.3.9 the full cost and risk implications for the Authority that would result from terminating the Soft LAN Services; 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 Soft LAN 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) 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 Soft LAN 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 Soft LAN 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

SCHEDULE 25 (Exit Management)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

requirements) of receipt of the Authority's notice of approval, a detailed Exit Plan in relation to the Soft LAN 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 Soft LAN Services based on the Supplier's knowledge and expertise;
 - 11.5.2 indicative cost estimates, applicable to the Soft LAN 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 Soft LAN 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 Soft LAN Services to be terminated;
 - 11.6.2 any Termination Assistance that the Authority requires;
 - 11.6.3 the date(s) on which the Soft LAN Services will terminate;
 - 11.6.4 the impact on the Charges with reference to the Charges that will cease from the date the Soft LAN Services terminate, and the new Charges in accordance with 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,

SCHEDULE 25 (Exit Management)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 Soft LAN 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 Soft LAN 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.

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;

- (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) NOT USED;
- (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;
- (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;
 - (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;
- (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.

ANNEX 2: (Draft Ethical Wall Agreement)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

ANNEX 2: DRAFT ETHICAL WALL AGREEMENT

[THE AUTHORITY]

and

[THE COUNTERPARTY]

ETHICAL WALL AGREEMENT

This Agreement is dated [] 20[] (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

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,
- (e) 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 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.

- 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 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;

- 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).

- 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 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.

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 will occur at 9.00am on the same Working	Properly addressed prepaid and delivered as evidenced by signature of a delivery receipt.

Manner of Delivery	Deemed time of service	Proof of service
	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 shall be governed by and construed in accordance with the laws of England and Wales.

ANNEX 2: (Draft Ethical Wall Agreement)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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:

ANNEX 3: GUIDANCE FOR EXIT PLAN**GUIDANCE FOR SUPPLIER CONTRACT EXIT PLAN**11th 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.
- 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 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]

**ANNEX 4: (Principles for Determining Charges, Costs and Expenses
in Relation to Exit and Termination Services)**

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

**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));

**ANNEX 4: (Principles for Determining Charges, Costs and Expenses
in Relation to Exit and Termination Services)**

Confidential

Security Classification (Official)

Contract for the provision of LAN Services

Contract reference: con_24092

- 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).

ANNEX 5: (Diagram of Exit Process)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

**ANNEX 5
DIAGRAM OF EXIT PROCESS**

NOTE: The diagram below has been included for illustration purposes only to summarise and illustrate the Partial Termination process for Soft LAN 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 26 (Service Continuity Plan and Corporate
Resolution Planning)**

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

SCHEDULE 26

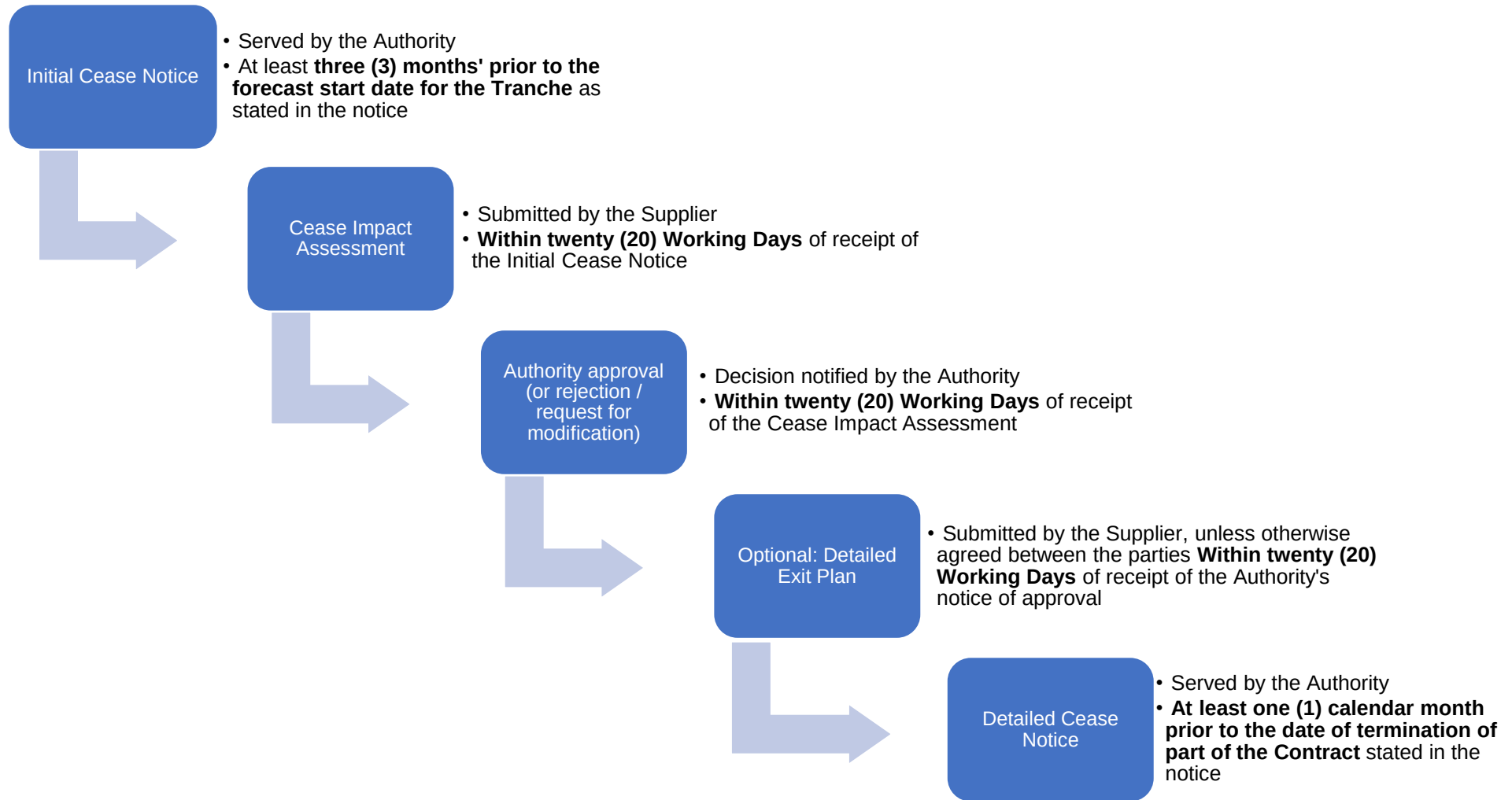
**SERVICE CONTINUITY PLAN AND CORPORATE
RESOLUTION PLANNING**

SCHEDULE 26 (Service Continuity Plan and Corporate Resolution Planning)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services



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: (c) Government Department; or (d) 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).

SCHEDULE 26 (Service Continuity Plan and Corporate Resolution Planning)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

“IT Service Continuity Management Plan”	means the plan prepared pursuant to Paragraph 2 of this Schedule which incorporates the ITSC 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 Vodafone, Atos and Xerox;
“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.

2.3 Following receipt of the draft IT Service Continuity Management Plan from the Supplier, the Authority shall:

SCHEDULE 26 (Service Continuity Plan and Corporate Resolution Planning)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- (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;
- (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

SCHEDULE 26 (Service Continuity Plan and Corporate Resolution Planning)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

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; and
- (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.

3.2 The IT Service Continuity Management Plan shall be designed so as to ensure that:

SCHEDULE 26 (Service Continuity Plan and Corporate Resolution Planning)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- (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.
- 4.2 The ITSC Plan shall:
- (a) address the various possible levels of failures of or disruptions to the Services;

SCHEDULE 26 (Service Continuity Plan and Corporate Resolution Planning)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN 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;
 - (vii) network planning including details of all relevant data networks and communication links;
 - (viii) invocation rules;

SCHEDULE 26 (Service Continuity Plan and Corporate Resolution Planning)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- (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;
 - (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;

SCHEDULE 26 (Service Continuity Plan and Corporate Resolution Planning)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN 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 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

SCHEDULE 26 (Service Continuity Plan and Corporate Resolution Planning)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

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.

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

SCHEDULE 26 (Service Continuity Plan and Corporate Resolution Planning)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

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.
- 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

SCHEDULE 26 (Service Continuity Plan and Corporate Resolution Planning)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

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;

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 reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- (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 (*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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- (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) Aa3 or better from Moody's; or
 - (b) AA- or better from Standard and Poor's; or
 - (c) AA- or better from Fitch;
- 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 disclosed and discussed that information with the Relevant Authority or Relevant Authorities, redact or omit that information from the CRP Information

SCHEDULE 26 (Service Continuity Plan and Corporate Resolution Planning)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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:

- (a) redacting only those parts of the information which are subject to such obligations of confidentiality

SCHEDULE 26 (Service Continuity Plan and Corporate Resolution Planning)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- (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.

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 reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

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 27 (Conduct of Claims)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 27
CONDUCT OF CLAIMS

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:

SCHEDULE 27 (Conduct of Claims)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (a) the Indemnifier is not entitled to take conduct of the Claim in accordance with Paragraph 1.3;
- (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

SCHEDULE 27 (Conduct of Claims)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

to bring a claim against the other Party pursuant to the indemnities in this Schedule.

SCHEDULE 28

STAFF TRANSFER

Schedule 28 (*Staff Transfer*)

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

“Admission Agreement”	as defined in Part A;
“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>

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 with such other information anonymised where possible. 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 to Part D of this Schedule;

“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;
“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 of any Sub-contractor 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*) and the following Annex may apply
 - (i) - Annex D1 (*CSPS*)
 - (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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

PART A: NOT USED

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 will 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

- (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 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 reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- (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 by the Authority prior to the Relevant Transfer Date 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 (as the case may be) may within 15 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 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 the relevant 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 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, 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 if required (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 and 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;

(b) the breach or non-observance by the Supplier or any Sub-contractor on or after the Relevant Transfer Date of:

SCHEDULE 28 (Staff Transfer)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- (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 in respect of, any Transferring Former Supplier Employee on or 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 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 any 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 and, 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 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) New Fair Deal.
- 5.2 Any changes embodied 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.

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 15 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 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 the relevant 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, (a) comply with such obligations as may be imposed upon it under Law and (b) comply with the provisions of Part D (Pensions) and its Annex of this Staff Transfer Schedule..
- 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 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 relevant Sub-contractor to the Authority within 6 months of the relevant Relevant Transfer Date.

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) the Transferring Former Supplier Employees;

- (b) those employees who are not Transferring Former Supplier Employees but to whom the Employment Regulations apply on the 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 Paragraph 2.5 of Part 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 or a Broadly Comparable pension scheme provided in accordance with Paragraph 10 of this Part D 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 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.

- 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) to 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 CSPA 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

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 and the Fund Actuary 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 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

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 Scheme(s);
- (b) consult with those Fair Deal Eligible 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 CSPA or the Authority may reasonably require, to enable the Replacement

Supplier to participate in the appropriate Statutory Scheme in respect of any Fair Deal Eligible Employees that remain eligible for New Fair Deal protection following a Service Transfer.

10 BROADLY COMPARABLE PENSION SCHEME ON RELEVANT TRANSFER DATE

Not used

11 BROADLY COMPARABLE PENSION SCHEME IN OTHER CIRCUMSTANCES

11.1 If the terms of Paragraph 2.2 of Annex D1: CSPS, apply, 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).

11.3 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):

- (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

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 the 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 to 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

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:

- (a) any unpaid employer's contributions or employee's contributions or any other financial obligations under the CSPA or any CSPA Admission Agreement in respect of the CSPA 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 Paragraph 12.1 above.

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 Principal Civil Service Pension Scheme 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; and "alpha" introduced under The Public Service (Civil Servants and Others) Pensions Regulations 2014.

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

SCHEDULE 28 (Staff Transfer)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

accrue benefits in the CSPA in accordance with the provisions governing the relevant 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.

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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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 to Part D (*Pensions*) of this Schedule 28 (Staff Transfer) (as appropriate); and

- (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) tax code;
 - (e) details of any voluntary deductions from pay; and
 - (f) bank/building society account details for payroll purposes.
- 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.

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 disappplied 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 in respect of the Transferring Supplier Employees arising under the Employment Regulations in respect of the period up to (and including) 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 all the Transferring Supplier Employees 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, accrued but untaken holiday pay, 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:
 - (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 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 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
- (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.

2.11 The Supplier shall comply, and shall procure that each Sub-contractor shall comply, with all its obligations under 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 any person identified in the Supplier's Final Supplier Personnel list up to (and including) the Service 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, pension contributions and all such sums due as a result of any Fair Deal Employees' participation in the Schemes and any requirement to set up a broadly comparable pension scheme and which in any case are attributable in whole or in part in respect of the period up to (and including) the Service Transfer Date) and any necessary apportionments in respect of any periodic payments shall be made between:

(a) the Supplier or any relevant Sub-contractor, as appropriate; and

SCHEDULE 28 (Staff Transfer)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

- (b) any Replacement Supplier or Replacement Sub-contractor, as appropriate.
- 2.12 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.
- 2.13 Subject to Paragraph 2.14, 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 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

SCHEDULE 28 (Staff Transfer)

Confidential

Contract reference: con_24092

Security Classification (Official)

Contract for the provision of LAN Services

Sub-contractor in relation to obligations under regulation 13 of the Employment Regulations.

- 2.14 The indemnities in Paragraph 2.13 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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

ANNEX E1: LIST OF NOTIFIED SUB-CONTRACTORS

SCHEDULE 28 (Staff Transfer)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

ANNEX E2: STAFFING INFORMATION

SCHEDULE 28 (Staff Transfer)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**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.

SCHEDULE 28 (Staff Transfer)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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							
Emp No							

SCHEDULE 28 (Staff Transfer)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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							
Emp No							

SCHEDULE 28 (Staff Transfer)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

	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								
Emp No								

SCHEDULE 28 (Staff Transfer)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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								

SCHEDULE 28 (Staff Transfer)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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						

SCHEDULE 28 (Staff Transfer)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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						

SCHEDULE 28 (Staff Transfer)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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

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 Roles	Name of Key Personnel	Responsibilities /Authorities	Phase of the project during which they will be a Member of Key Personnel	Minimum Period in Key Role
Service Manager	Phil Redhead	Proactively manages service performance against agreed SLAs. • The Supplier’s lead at the Service Review and Operational Review Board. • Escalation point for service issues. • Provides a comprehensive monthly Performance Reporting Pack to support the service review. • Contributes to service strategy. • Proactive identification, ownership, and delivery of operational service improvements. • Responding to customer satisfaction surveys and complaints. • Manage CI plans	Contract Duration	3 Months
Project Manager	Ashley Lamb	• Develop project specifications, agree Project Plan baseline, key activities,	Transition and Implementation Phase	3 Months

SCHEDULE 29 (Key Personnel)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

		deliverables, resource requirements, milestones, and deadlines. • Utilise project plans and schedules to monitor and manage all activities		
Exit & Transition Manager	Ashley Lamb	• Accountable for the exit and transition strategy of the contract. • Responsible for the orderly exit of the in-scope IT services on expiry of the contracted service agreements following the successful transition of the services. • Builds a strong relationship with senior customer stakeholders. • Is the main interface and lead for the managed contract on all contractual/ commercial topics. • For the lifetime of the contract, monitors and manages contractual obligations including T&Cs and SLAs, through to exit of the contract. • Identifies and manages commercial risk. • Determines effective Change Control, immediately identifies a change to a contractual agreement and	Transition and Implementation Phase	3 Months

SCHEDULE 29 (Key Personnel)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

		ensures this is managed in the defined way/process. Independently maintains records for complex decision points, financial performance, service delivery, billing, efficiency of change controls and general support activities in relation to the contract.		
Test Manager	Sowmya Nandakumar	- A Single Point of Contact for testing communications and control and responsible for: - Test resource management and mobilisation. - Test Document production and review inclusive of customer calls, walkthroughs, and request for change. - Test Schedule production. - Test Checkpoint and Highlight reporting. - Test Risk mitigation and management. - Test obligation tracking.	Contract Duration	3 Months
Single Point of Contact for the IT Service Continuity Management Plan	Phil Redhea	Responsible for planning and performing the value chain activities required to deliver Service Continuity Management and: Contributing to the service strategy by identifying efficiencies through optimisation and automation.	Contract Duration	3 Months

SCHEDULE 29 (Key Personnel)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

		• A key interface to ensure contract requirements and expectations met. • Collaborating with other ITIL practices ensuring contract obligations are met. • Planning, agreeing, and managing a program of DR testing. • Ensuring documentation is produced and reviewed in line with contract requirements. • Identifying CSI activities and driving through to completion. • Internal and external audits demonstrating governance and compliance with ISO20000, ISO27001, ISO22301 standards and any other relevant regulations.		
Security Representative	Josh Lucas	Responsible for: • identifying and managing security risks for the LAN Services. • Working with the relevant service teams to deliver the requirements on security testing for the Authority. • Working with the Authority Assurer to ensure that they have the necessary information to meet	Contract Duration	3 Months

SCHEDULE 29 (Key Personnel)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

		the assurance requirements.		

SCHEDULE 30 (Deed of Guarantee)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Schedule 30

DEED OF GUARANTEE

SCHEDULE 30 (Deed of Guarantee)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Note: The Authority does not require the Deed of Guarantee to be entered into at the Effective Date, however the Authority reserves the right to require a Guarantee to be provided as reasonably determined by the Authority during the Term in the form as detailed in this Schedule.

Schedule 30 (Deed of Guarantee)

[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:

"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: (d) by means of the holding of shares or the possession of voting power in relation to that body or any other body corporate; or (e) 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;

- (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**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:

- (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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- (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;
 - (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]

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.

SCHEDULE 30 (Deed of Guarantee)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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.

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.

SCHEDULE 30 (Deed of Guarantee)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 31

PROCESSING PERSONAL DATA

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 is

cpo@bt.com
The Group DPO
pp Floor 16
One Braham
1 Braham Street
London E1 8EE
- 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 <i>this Contract</i>). • Where the Supplier has professional or regulatory obligations in respect of the Personal Data received. • For billing and contract administration. • 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 LAN Services as described in the Contract and Schedule 2 specifically.

SCHEDULE 31 (Processing Personal Data)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Duration of the processing	The Term and (to the extent relevant) the Termination Assistance Period.
Nature, and purposes 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. The purpose of the processing is to provide and operate the Controller Services. Processing of business contact information (contact details, phone numbers and business addresses). Storage of business contact information for RFSs (request for service) in the incumbent suppliers database. Site details about asset, circuits and configuration items held in CMDB in the incumbent supplier and MoJ in ServiceNow system (the "Controller Services").
Type of Personal Data	Staff and user personal data including but not limited to: • IP addresses • Device hostnames and nicknames • User names (login credentials) • Business Contact Details • Business Contact Information • Access logs • Customer records
Categories of Data Subject	Categories of Data Subject may include: 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	Please see the list of Subcontractors and their locations in Appendix 7. BT will process personal data in key locations within the UK.

SCHEDULE 31 (Processing Personal Data)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Protective Measures that the Supplier and, where applicable, its Sub-contractors have implemented 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	All BT personnel with access to Personal Data under this Contract will be UK based and SC cleared. All BT UK personnel are required to comply with UK GDPR and UK Data Protection Act 2018. Everyone in BT has Data Protection responsibilities and is required undergo annual training with an associated test for which achieving a pass mark is mandatory. Data security underpins our approach to Data Protection, and our structured approach to security starts with a high-level policy set based on International Security Standards, which are modelled after ISO27001 and is supported by working practices, technical standards and a network of security professionals in functional organisations throughout the business. BT will deliver and support the service from service desks that have ISO27001 certification, and that will have Cyber Essentials PLUS certification prior to being approved to handle Authority Data. Additionally, all our services have been subject to security testing, and those components that are dedicated to the Authority will be subject to CHECK testing prior to being approved to handle Authority Data. These measures will be maintained throughout the programme. BT has a Data Privacy Team, consisting of specialists in data protection, including lawyers, who are available to provide support for new and existing business and who can liaise with the Authority to ensure that appropriate measures that meet data protection regulations are implemented. We would refer the Authority to Annex 4 and Schedule 5 which sets out further details around the protective measures to protect personal data that BT will adhere to. All Subcontractors will be required to comply with the provisions of clause 21 of the Core Terms where they are processing personal data as a Data Processor.

SCHEDULE 31 (Processing Personal Data)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

ANNEX 1: NOT USED

ANNEX 2: NOT USED

ANNEX 3: NOT USED

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 otherwise makes accessible any Shared Personal Data to the other party (or any person acting on the other party's behalf);

Permitted Lawful Basis

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

SCHEDULE 31 (Processing Personal Data)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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; (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);
Processor	has the meaning given in Data Protection Legislation;
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 special categories of Personal Data as referred to in Data Protection Legislation.

2 Status of the Parties

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.
- 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 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 3;

- 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 to Process the Shared Personal Data for the Permitted Purpose in accordance with the terms of this Contract;
- 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:

- (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 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

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.

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 The Parties each agree to provide such assistance as is reasonably required to enable the other Party to comply with Data Subject Requests within the time limits imposed by the Data Protection Legislation. If such contact from a Data Subject relates to the other Party's Processing, then the Receiving Party will promptly (and in any event within two (2) Working Days) pass it onto the other Party to manage.
- 9.3 Not used.
- 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 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 Shared 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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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

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

The Parties shall comply with and maintain, the arrangements set out in Appendix 5 of this Annex 4.

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 Schedule 31 and Clause 21;

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 Schedule 31 and Clause 21; 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

SCHEDULE 31 (Processing Personal Data)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 one month 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, each Party will not retain the Received Personal Data for longer than is necessary to fulfil the Contract and any obligations to retain the Received Personal Data under applicable Law.

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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Appendix 1

How the Shared Personal Data will be shared

NOT USED

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 local area network (LAN) 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 LAN services in the justice system.

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 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

SCHEDULE 31 (Processing Personal Data)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Appendix 4
Transparency arrangements

NOT USED

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:

cpo@bt.com
The Group DPO,
pp Floor 16
One Braham
1 Braham Street
London E1 8EE

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 by this Schedule 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 Relationship between Contact Points**3.1** The Contact Points of each party shall meet, by phone if necessary, not less than *once every month* to manage the relationship between the parties and assess:

3.1.1 the overall effectiveness of the sharing arrangements set out in this Schedule;

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

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;
 - 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

SCHEDULE 31 (Processing Personal Data)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**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]	[REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED]	[REDACTED]	[REDACTED] [REDACTED]

SCHEDULE 32 (Intellectual Property Rights)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

Schedule 32

INTELLECTUAL PROPERTY RIGHTS

Schedule 32 (*Intellectual Property Rights*)

1 INTELLECTUAL PROPERTY RIGHTS

1.1 Except as expressly set out in this Contract:

- (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 Supplier Software;
 - (ii) the Third Party Software;
 - (iii) the Third Party IPRs; and
 - (iv) the Supplier 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) Specially Written Software and 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 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 Specially Written Software and Project Specific IPRs in Annex 1 to this Schedule 32 (*Intellectual Property Rights*) and shall keep Annex 1 updated during the Term.

2 TRANSFER AND LICENCES GRANTED BY THE AUTHORITY AND THE SUPPLIER

Specially Written Software and Project Specific IPRs

- 2.1 Subject to Paragraph 2.17 (*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) (*Intellectual Property Rights*)) not already resting with the Supplier in the Specially Written Software and the Project Specific IPRs including (without limitation):
- (a) the Documentation, Source Code and the Object Code of the 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 Specially Written Software (together the “**Software Supporting Materials**”).
- 2.2 The Authority shall execute all such assignments as are required to ensure that any rights in the Specially Written Software and Project Specific IPRs are properly transferred to the Supplier.
- 2.3 If within three years of its creation, any Intellectual Property in the Specially Written Software and/or the 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 Specially Written Software and/or the Project Specific IPRs to the Authority. Each party shall bear its own costs in such assignment.

Supplier Software, Specially Written Software, Project Specific IPRs, and Supplier Background IPRs

- 2.4 The Supplier shall not use any Supplier Non-COTS Software or Supplier Non-COTS Background IPR in the provision of the Services unless it is detailed in Schedule 12 (*Software*); or sent to the Enterprise Architecture Board for review and approval granted by the Authority. Prior to the use of any Supplier Non-COTS Software or Supplier Non-COTS Background IPR in the provision of the Services, the Supplier shall notify the Authority in writing giving details of any Know-How, trade secrets or Confidential Information contained in the Supplier Non-COTS Software or Supplier Non-COTS Background IPR and whether there are any restrictions on its use which are inconsistent with any of the rights and licences granted to the Authority and the Service Recipients under this Schedule.
- 2.5 The Supplier hereby grants to the Authority and the Service Recipients:
- (a) subject to the provisions of Paragraph 2.18 (*Patents*) and Clause 32.11 (b) (*Consequences of expiry or termination*), 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 Supplier Non-COTS Software for which the Supplier delivers a copy to the Authority for any purpose relating to the 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) the Supplier Non-COTS Background IPRs, the Specially Written Software and the Project Specific IPRs for any purpose relating to the 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 Supplier COTS Software for which the Supplier delivers a copy to the Authority and Supplier COTS Background IPRs on the licence terms identified in a letter in or substantially in the form set out in Annex 1 to Schedule 12 (*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 Supplier COTS Software and Supplier COTS Background IPRs on equivalent terms to those set out in Paragraphs 2.8 (*Authority's right to sub-license*) and 2.9 (*Authority's and Service Recipient's right to assign/novate sub-licences*) in relation to the Supplier Non-COTS Software and Supplier Non-COTS Background IPRs; and
 - (c) a perpetual royalty-free non-exclusive licence to use without limitation any Know-How, trade secrets or Confidential Information contained within the Specially Written Software or the Project Specific IPRs.
- 2.6 At any time during the Term or following termination or expiry of this Contract, the Supplier may terminate the licence granted in respect of the Supplier Non-COTS Software under Paragraph 2.5(a)(i) or in respect of the Supplier 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 (*Authority's right to sub-license*) commits any material breach of the terms of Paragraph 2.5(a)(i) or 2.5(a)(ii) or 2.8(a)(ii) (as the case may be) which, if the breach is 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 Supplier Non-COTS Software or the Supplier Non-COTS Background IPRs is terminated pursuant to Paragraph 2.6, the Authority shall:
- (a) immediately cease all use of the Supplier Non-COTS Software or the Supplier 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 Supplier Non-COTS Software and/or the Supplier 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 Supplier Non-COTS Software and/or the Supplier Non-COTS Background IPRs (as the case may be); and
- (c) ensure, so far as reasonably practicable, that any Supplier Non-COTS Software and/or Supplier 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) from any computer, word processor, voicemail system or any other device containing such Supplier Non-COTS Software and/or Supplier Non-COTS Background IPRs.

Authority's right to sub-license

2.8 Subject to Paragraph 2.18 (*Patents*) the Authority may sub-license:

- (a) the rights granted under Paragraph 2.5(a) (*Supplier Software, Specially Written Software, Project Specific IPRs and Supplier 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) (*Supplier Software, Specially Written Software, Project Specific IPRs and Supplier Background IPRs*) only for purposes relating to the 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 Annex 2 to Schedule 12 (*Software and*
- (b) the rights granted under Paragraph 2.5(a) (*Supplier Software, Specially Written Software, Project Specific IPRs and Supplier Background IPRs*) to any Approved Sub-Licensee to the extent necessary to use and/or obtain the benefit of the Specially Written Software and/or the 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 Annex 2 to Schedule 12 (*Software*) duly executed by the Approved Sub-Licensee.

Authority's and Service Recipient's 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) (*Supplier Software, Specially Written Software, Project Specific IPRs and Supplier 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 been performed and/or carried on by the Authority.
- 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 (*Supplier Software, Specially Written Software, Project Specific IPRs and Supplier 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 (*Supplier Software, Specially Written Software, Project Specific IPRs and Supplier Background IPRs*).
- 2.11 If a licence granted in Paragraph 2.5 (*Supplier Software, Specially Written Software, Project Specific IPRs and Supplier Background IPRs*) is novated under Paragraph 2.9 (*Authority's and Service Recipient's 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.

Third Party Software and Third Party IPRs

- 2.12 The Supplier shall not use in the provision of the Services (including in any Specially Written Software or in the software element of Project Specific IPRs) any Third Party Non-COTS Software or Third Party Non-COTS IPRs unless detailed in Schedule 12 (*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 Authority on a royalty-free basis to the Authority 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 (*Supplier Software,*

Specially Written Software, Project Specific IPRs and Supplier Background IPRs) and Paragraph 2.9 (Authority's and Service Recipient's 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 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 the Contract 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 20 Working Days of notification pursuant to Paragraph 2.13(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 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 Specially Written Software and/or the 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 ten (10) days of what those rights are and which parts of the Specially Written Software and the Project Specific IPRs they are found in.

Termination and Replacement Suppliers

2.16 For the avoidance of doubt, the termination or expiry of this Contract 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.

2.17 The Supplier shall, if requested by the Authority in accordance with Schedule 25 (*Exit Management*) and at the Supplier's cost:

- (a) grant (or procure the grant) to any Replacement Supplier of:
 - (i) a licence to use any Supplier Non-COTS Software, Supplier Non-COTS Background IPRs, Third Party Non-COTS IPRs, Specially Written Software, 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 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 Annex 2 to Schedule 12 (*Software*); duly executed by the Replacement Supplier;
 - (ii) a licence to use any Supplier COTS Software and/or Supplier 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.

Patents

2.18 Where a patent owned by the Supplier is necessarily infringed by the use of the Specially Written Software or Project Specific IPRs by the Authority, the Service Recipients or any Replacement Supplier, the Supplier hereby grants to 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 Contract.

3 LICENCES GRANTED BY THE AUTHORITY

- 3.1 The Authority hereby grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Term to use the Authority Software, the Authority Background IPRs and the Authority Data solely to the extent necessary for performing the Services in accordance with this Contract, 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 Clause 22 (*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.
- 3.2 In the event of the termination or expiry of this Contract, the licence granted pursuant to Paragraph 3.1 and any sub-licence granted by the Supplier in accordance with Paragraph 3.1 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, return or destroy documents and other tangible materials that contain any of the Authority Software, the Authority Background IPRs and 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 the Authority Data (as the case may be); and
 - (a) ensure, so far as reasonably practicable, that any Authority Software, Authority Background IPRs and 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.
- 3.3 The Supplier may use and exploit the Specially Written Software and/or the Project Specific IPRs provided that:
- (a) the Supplier must always offer a price and solution to the Authority which is in accordance with the Charges;
 - (b) where the Supplier proposes to exploit the Specially Written Software and/or the Project Specific IPRs, that it provides a detailed proposal of its plans for exploitation of the Specially Written Software and/or the 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 Specially Written Software and/or the 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 the Contract; and any other information that would reasonably be required by the Authority to enable it 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 Specially Written Software and/or the Project Specific IPRs, that it provides clear evidence to demonstrate how the exploitation plans and financial information provided under Paragraph 3.3(b) above have been applied to the price for the Deliverables offered to the Authority and other potential users;

- 3.4 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.

SCHEDULE 32 (Intellectual Property Rights)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**ANNEX 1: SPECIALLY WRITTEN SOFTWARE AND PROJECT SPECIFIC IPRS**

Name of Specially Written Software and Project Specific IPRs	Details

SCHEDULE 33 (Service Recipients)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

SCHEDULE 33
SERVICE RECIPIENTS

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 person named as such in the Annex 1 to this Schedule 33 (Service Recipients);

“Potential Service Recipients” means a person named as such in Annex 2 to this Schedule 33 (Service Recipients); and

“Service Recipients” means:

- (a) the Initial Service Recipients; and
- (b) any:
 - (I) Potential Service Recipients;
 - (II) arms' length bodies of the Authority;
 - (III) body (including any private sector body) created or formed, or brought within the Authority's responsibility or control, after the date of this Contract; or
 - (IV) 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.

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.

SCHEDULE 33 (Service Recipients)

Confidential

Contract reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services

- 3.2 The Initial Service Recipients who are to benefit under the Contract are identified in Annex A to this Schedule 33 (Service Recipients). Additional Service Recipients shall be added to the list in Annex A 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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**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 Procedure Rule Committee
Criminal Injuries Compensation Authority (CICA)
Family Justice Council
Family Procedure Rule Committee
Government Facilities Services Ltd (GFSL)
His Majesty's Courts and Tribunal 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 Prisons and Probation Service (HMPPS)
Independent Advisory Panel on Deaths in Custody
Independent Monitoring Authority (IMA) for the Citizens' Rights Agreements
Independent Monitoring Boards (IMB)
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 reference: con_24092

Security Classification (Official)
Contract for the provision of LAN Services**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)