

Direct Award Order Form

CALL-OFF REFERENCE: CQC I&D 143

THE BUYER: Care Quality Commission (URN: 10025944)

BUYER ADDRESS Citygate, Gallowgate, Newcastle Upon Tyne
NE1 3PA

SUPPLIER REFERENCE RM6116-0221

THE SUPPLIER: Vodafone Limited

SUPPLIER ADDRESS: Vodafone House, The Connection, Newbury,
Berkshire RG14 2FN

REGISTRATION NUMBER: 01471587

DUNS NUMBER: 226488435

SID4GOV ID: Not Applicable

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated the date of issue.

It's issued under the Framework Contract with the reference number RM6116 for the provision of Network Services.

CALL-OFF LOT(S):

Lot 1a Inter site Connectivity (Wide Area Network) / Data Access Services

Lot 2a Intra site Connectivity (Local Area Network) / Local Connectivity Services

CALL-OFF INCORPORATED TERMS

The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form, including the Call-Off Special Terms and Call-Off Special Schedules.

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

2. Joint Schedule 1 (Definitions and Interpretation) RM6116
3. Framework Special Terms
4. The following Schedules in equal order of precedence:
 - Joint Schedules for RM6116
 - Joint Schedule 2 (Variation Form)
 - Joint Schedule 3 (Insurance Requirements)
 - Joint Schedule 4 (Commercially Sensitive Information)
 - Joint Schedule 10 (Rectification Plan)
 - Joint Schedule 11 (Processing Data)
 - Call-Off Schedules for RM6116
 - Call-Off Schedule 1 (Transparency Reports)
 - Call-Off Schedule 2 (Staff Transfer)
 - Call-Off Schedule 3 (Continuous Improvement)
 - Call-Off Schedule 5 (Pricing Details)
 - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
 - Call-Off Schedule 9 (Security)
 - Call-Off Schedule 11 (Installation Works)
 - Call-Off Schedule 14 (Service Levels)
 - Call-Off Schedule 20 (Call-Off Specification)
5. CCS Core Terms (version 3.0.11)
6. Joint Schedule 5 (Corporate Social Responsibility) RM6116

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS

The following Special Terms are incorporated into this Call-Off Contract:

Special Term 1 - Global Supply Chain and Distribution

Buyer accepts that the impacts on global supply and distribution are beyond Supplier's control and may affect the performance of its obligations under the Call-Off Contract. Where, as a result of global supply and distribution impacts beyond Supplier's control, Supplier cannot meet any (a) Milestone Date or agreed delivery dates (for Deliverables) or needs to adjust implementation or installation plans, or (b) relevant service levels (or similar Service performance criteria), it is relieved of any accompanying liability or obligations under the terms of the Call-Off Contract.

CALL-OFF START DATE: 21/07/2025

CALL-OFF EXPIRY DATE: Shall be 24 months from the Call-Off Start Date

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

CALL-OFF INITIAL PERIOD: Shall be 24 months from the Call-Off Start Date

CALL-OFF OPTIONAL EXTENSION PERIOD Not Applicable

MINIMUM PERIOD OF NOTICE FOR WITHOUT REASON TERMINATION

The Buyer may terminate this Call-Off Contract at any time by giving the Supplier not less than 90 days' prior written notice.

CATALOGUE SERVICE OFFER REFERENCE

RM6116-Lot1a-VodafoneLtd-#071 ; RM6116-Lot1a-VodafoneLtd-#070 ; RM6116-Lot2a-VodafoneLtd-#020

CALL-OFF DELIVERABLES VIA *DIRECT AWARD*

Deliverable 1: IPVPN Primary – Newcastle Gallowgate NE1 4WH; Quantity: 1

Deliverable 2: IPVPN Secondary – Newcastle Gallowgate NE1 4WH; Quantity: 1

Deliverable 3: IPVPN Primary – Stratford E20 1JQ; Quantity: 1

Deliverable 4: IPVPN Secondary – Stratford E20 1JQ; Quantity: 1

Deliverable 5: IPVPN Primary – Manchester Computacenter UK – M50 2UW; Quantity: 1

Deliverable 6: IPVPN Primary – Bristol BS1 6PN; Quantity: 1

Deliverable 7: IPVPN Primary – Nottingham NG2 4LA; Quantity: 1

Deliverable 8: Secure Network Gateway – Enhanced Network Based Internet Access; Quantity: 1

Deliverable 9: Secure Network Gateway – Demilitarized Zone Optional Add-on; Quantity: 1

Deliverable 10: Microsoft Cloud Connect; Quantity: 1

Deliverable 11: TSSM, CTL and Capacity Manager; Quantity: 1

Deliverable 12: DIA Primary – Newcastle City Gate; Quantity: 1

Deliverable 13: DIA Secondary – Newcastle City Gate; Quantity: 1

Deliverable 14: DIA Primary – Stratford Redman Place; Quantity: 1

Deliverable 15: DIA Secondary – Stratford Redman Place; Quantity: 1

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

Deliverable 16: LAN Maintenance; Quantity: 1

Deliverable 17: LAN Monitoring; Quantity: 1

Deliverable 18: LAN Management; Quantity: 1

Deliverable 19: Meraki Wi-Fi Maintenance; Quantity: 1

Deliverable 20: Cisco Identity Services Engine (ISE) Maintenance; Quantity: 1

See details in Call-Off Schedule 20 (Call-Off Specification).

The Expiry Date for Deliverables 16 to 20 (inclusive) shall be 12 months from the Call-Off Start Date. The Expiry Date for all other Deliverables shall be the Call-Off Expiry Date.

Buyer acknowledges and accepts that it is aware of the Supplier's press release published [Is your business ready for the PSTN switch-off? \(vodafone.co.uk\)](https://www.vodafone.co.uk/news/your-business-ready-for-the-pstn-switch-off) and CCS publication [Crown Commercial Service publication in relation to PSTN](#). Openreach, KCOM and Virgin Media will switch off PSTN (Public Switched Telephone Network) in January 2027, or other date as may be published or notified by third party provider. Buyer will proactively and without delay, observe and comply with Buyer's obligations in connection with changes to Services necessary to address legacy service technologies and in particular, Buyer undertakes to address the resulting impact and compatibility of any Deliverables or buyer equipment in connection with the Service provided by the Supplier.

MAXIMUM LIABILITY

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges (excluding VAT) used to calculate liability in the first Contract Year is £346,505.09.

CALL-OFF CHARGES

Deliverable 1: IPVPN Primary – Newcastle Gallowgate NE1 4WH; Quantity: 1;
Charge per unit (e.g. per connection or licence):

[REDACTED]

Deliverable 2: IPVPN Secondary – Newcastle Gallowgate NE1 4WH; Quantity: 1;
Charge per unit (e.g. per connection or licence):

[REDACTED]

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

Deliverable 3: IPVPN Primary – Stratford E20 1JQ; Quantity: 1; Charge per unit (e.g. per connection or licence): [REDACTED]

Deliverable 4: IPVPN Secondary – Stratford E20 1JQ; Quantity: 1; Charge per unit (e.g. per connection or licence): [REDACTED]

Deliverable 5: IPVPN Primary – Manchester Computacenter UK – M50 2UW; Quantity: 1; Charge per unit (e.g. per connection or licence): [REDACTED]

Deliverable 6: IPVPN Primary – Bristol BS1 6PN; Quantity: 1; Charge per unit (e.g. per connection or licence): [REDACTED]

Deliverable 7: IPVPN Primary – Nottingham NG2 4LA; Quantity: 1; Charge per unit (e.g. per connection or licence): [REDACTED]

Deliverable 8: Secure Network Gateway – Enhanced Network Based Internet Access; Quantity: 1; [REDACTED]

Deliverable 9: Secure Network Gateway – Demilitarized Zone Optional Add-on; Quantity: 1; [REDACTED]

Deliverable 10: Microsoft Cloud Connect; Quantity: 1; [REDACTED]

Deliverable 11: TSSM, CTL and Capacity Manager; Quantity: 1; Charge per unit: [REDACTED]

Deliverable 12: DIA Primary – Newcastle City Gate; Quantity: 1; Charge per unit (e.g. per connection or licence): [REDACTED]

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

Deliverable 13: DIA Secondary – Newcastle City Gate; Quantity: 1; Charge per unit (e.g. per connection or licence): [REDACTED]

Deliverable 14: DIA Primary – Stratford Redman Place; Quantity: 1; [REDACTED]

Deliverable 15: DIA Secondary – Stratford Redman Place; Quantity: 1; Charge per unit (e.g. per connection or licence): [REDACTED]

Deliverable 16: LAN Maintenance; Quantity: 1; [REDACTED]

Deliverable 17: LAN Monitoring; Quantity: 1; [REDACTED]

Deliverable 18: LAN Management; Quantity: 1; Charge per unit: [REDACTED]

Deliverable 19: Meraki Wi-Fi Maintenance; Quantity: 1; Charge per unit: [REDACTED]

Deliverable 20: Cisco Identity Services Engine (ISE) Maintenance; Quantity: 1; Charge per unit: [REDACTED]

See details in Call-Off Schedule 5 (Pricing Details).

All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4, 5 and 6 (if used) in Framework Schedule 3 (Framework Prices). The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of:

- Indexation
- Specific Change in Law

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2018

As permitted under paragraph 1.2 of Part A of Framework Schedule 3, the Supplier and Buyer hereby agree that in April of each calendar year, all Charges will increase by a percentage equal to the percentage increase in the UK Consumer Price Index ("CPI") published by the Office for National Statistics (or any other body to which the functions of that office may be transferred) in January of that year compared to the previous year ("CPI Rate").

REIMBURSABLE EXPENSES

None

PAYMENT METHOD

BACS

BUYER'S INVOICE ADDRESS:

Care Quality Commission, First Floor, T70 Payables, Phoenix House, 5 Topcliffe Lane, Wakefield, West Yorkshire, WF3 1WE

[REDACTED]

BUYER'S ENVIRONMENTAL POLICY

Not applicable

BUYER'S SECURITY POLICY

Not applicable

SUPPLIER'S AUTHORISED REPRESENTATIVE

[REDACTED]

SUPPLIER'S CONTRACT MANAGER

[REDACTED]

PROGRESS REPORT FREQUENCY

Once, one month after the Call-Off Start Date.

PROGRESS MEETING FREQUENCY

Framework Ref: RM6116
Project Version: vFinal1.1
Model Version: v3.8

Framework Schedule 6 (Order Form Template and Call-Off Schedules)
Crown Copyright 2018

Once, one month after the Call-Off Start Date.

KEY STAFF

Not applicable

KEY SUBCONTRACTORS

See list of Key Subcontractors set out in each Service Offer within Call-Off Schedule 20 (Call-Off Specification)

COMMERCIALLY SENSITIVE INFORMATION

Supplier’s Commercially Sensitive Information

SERVICE CREDITS

Service Credits will accrue in accordance with Call-Off Schedule 14 (Service Levels).

ADDITIONAL INSURANCES

Not applicable

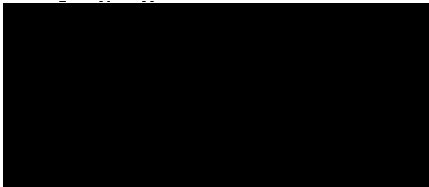
GUARANTEE

Not applicable

SOCIAL VALUE COMMITMENT

Not applicable

For and on behalf of the Supplier:	For and on behalf of the Buyer:
<div></div>	





Crown
Commercial
Service

Core Terms

1. Definitions used in the contract

Interpret this Contract using Joint Schedule 1 (Definitions).

2. How the contract works

- 2.1 The Supplier is eligible for the award of Call-Off Contracts during the Framework Contract Period.
- 2.2 CCS does not guarantee the Supplier any exclusivity, quantity or value of work under the Framework Contract.
- 2.3 CCS has paid one penny to the Supplier legally to form the Framework Contract. The Supplier acknowledges this payment.
- 2.4 If the Buyer decides to buy Deliverables under the Framework Contract it must use Framework Schedule 7 (Call-Off Award Procedure) and must state its requirements using Framework Schedule 6 (Order Form Template and Call-Off Schedules). If allowed by the Regulations, the Buyer can:
 - (a) make changes to Framework Schedule 6 (Order Form Template and Call-Off Schedules);
 - (b) create new Call-Off Schedules;
 - (c) exclude optional template Call-Off Schedules; and/or
 - (d) use Special Terms in the Order Form to add or change terms.
- 2.5 Each Call-Off Contract:
 - (a) is a separate Contract from the Framework Contract;
 - (b) is between a Supplier and a Buyer;
 - (c) includes Core Terms, Schedules and any other changes or items in the completed Order Form; and
 - (d) survives the termination of the Framework Contract.
- 2.6 Where the Supplier is approached by any Other Contracting Authority requesting Deliverables or substantially similar goods or services, the Supplier must tell them about this Framework Contract before accepting their order.
- 2.7 The Supplier acknowledges it has all the information required to perform its obligations under each Contract before entering into a Contract. When information is provided by a Relevant Authority no warranty of its accuracy is given to the Supplier.
- 2.8 The Supplier will not be excused from any obligation, or be entitled to additional Costs or Charges because it failed to either:
 - (a) verify the accuracy of the Due Diligence Information; or
 - (b) properly perform its own adequate checks.
- 2.9 CCS and the Buyer will not be liable for errors, omissions or misrepresentation of any information.

- 2.10 The Supplier warrants and represents that all statements made and documents submitted as part of the procurement of Deliverables are and remain true and accurate.

3. What needs to be delivered

3.1 All deliverables

- 3.1.1 The Supplier must provide Deliverables:

- (a) that comply with the Specification, the Framework Tender Response and, in relation to a Call-Off Contract, the Call-Off Tender (if there is one);
- (b) to a professional standard;
- (c) using reasonable skill and care;
- (d) using Good Industry Practice;
- (e) using its own policies, processes and internal quality control measures as long as they do not conflict with the Contract;
- (f) on the dates agreed; and
- (g) that comply with Law.

- 3.1.2 The Supplier must provide Deliverables with a warranty of at least 90 days from Delivery against all obvious defects.

3.2 Goods clauses

- 3.2.1 All Goods delivered must be new, or as new if recycled, unused and of recent origin.
- 3.2.2 All manufacturer warranties covering the Goods must be assignable to the Buyer on request and for free.
- 3.2.3 The Supplier transfers ownership of the Goods on Delivery or payment for those Goods, whichever is earlier.
- 3.2.4 Risk in the Goods transfers to the Buyer on Delivery of the Goods, but remains with the Supplier if the Buyer notices damage following Delivery and lets the Supplier know within 3 Working Days of Delivery.
- 3.2.5 The Supplier warrants that it has full and unrestricted ownership of the Goods at the time of transfer of ownership.
- 3.2.6 The Supplier must deliver the Goods on the date and to the specified location during the Buyer's working hours.
- 3.2.7 The Supplier must provide sufficient packaging for the Goods to reach the point of Delivery safely and undamaged.
- 3.2.8 All deliveries must have a delivery note attached that specifies the order number, type and quantity of Goods.
- 3.2.9 The Supplier must provide all tools, information and instructions the Buyer needs to make use of the

Core Terms

Goods.

- 3.2.10 The Supplier must indemnify the Buyer against the costs of any Recall of the Goods and give notice of actual or anticipated action about the Recall of the Goods.
- 3.2.11 The Buyer can cancel any order or part order of Goods which has not been Delivered. If the Buyer gives less than 14 days notice then it will pay the Supplier's reasonable and proven costs already incurred on the cancelled order as long as the Supplier takes all reasonable steps to minimise these costs.
- 3.2.12 The Supplier must at its own cost repair, replace, refund or substitute (at the Buyer's option and request) any Goods that the Buyer rejects because they do not conform with Clause 3. If the Supplier does not do this it will pay the Buyer's costs including repair or re-supply by a third party.

3.3 Services clauses

- 3.3.1 Late Delivery of the Services will be a Default of a Call-Off Contract.
- 3.3.2 The Supplier must co-operate with the Buyer and third party suppliers on all aspects connected with the Delivery of the Services and ensure that Supplier Staff comply with any reasonable instructions.
- 3.3.3 The Supplier must at its own risk and expense provide all Supplier Equipment required to Deliver the Services.
- 3.3.4 The Supplier must allocate sufficient resources and appropriate expertise to each Contract.
- 3.3.5 The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer's operations, employees or other contractors.
- 3.3.6 The Supplier must ensure all Services, and anything used to Deliver the Services, are of good quality and free from defects.
- 3.3.7 The Buyer is entitled to withhold payment for partially or undelivered Services, but doing so does not stop it from using its other rights under the Contract.

4. Pricing and payments

- 4.1 In exchange for the Deliverables, the Supplier must invoice the Buyer for the Charges in the Order Form.
- 4.2 CCS must invoice the Supplier for the Management Charge and the Supplier must pay it using the process in Framework Schedule 5 (Management Charges and Information).
- 4.3 All Charges and the Management Charge:
- (a) exclude VAT, which is payable on provision of a valid VAT invoice; and
 - (b) include all costs connected with the Supply of Deliverables.
- 4.4 The Buyer must pay the Supplier the Charges within 30 days of receipt by the Buyer of a valid,

Core Terms

undisputed invoice, in cleared funds using the payment method and details stated in the Order Form.

4.5 A Supplier invoice is only valid if it:

- (a) includes all appropriate references including the Contract reference number and other details reasonably requested by the Buyer;
- (b) includes a detailed breakdown of Delivered Deliverables and Milestone(s) (if any); and
- (c) does not include any Management Charge (the Supplier must not charge the Buyer in any way for the Management Charge).

4.6 The Buyer must accept and process for payment an undisputed Electronic Invoice received from the Supplier.

4.7 The Buyer may retain or set-off payment of any amount owed to it by the Supplier if notice and reasons are provided.

4.8 The Supplier must ensure that all Subcontractors are paid, in full, within 30 days of receipt of a valid, undisputed invoice. If this does not happen, CCS or the Buyer can publish the details of the late payment or non-payment.

4.9 If CCS or the Buyer can get more favourable commercial terms for the supply at cost of any materials, goods or services used by the Supplier to provide the Deliverables, then CCS or the Buyer may require the Supplier to replace its existing commercial terms with the more favourable terms offered for the relevant items.

4.10 If CCS or the Buyer uses Clause 4.9 then the Framework Prices (and where applicable, the Charges) must be reduced by an agreed amount by using the Variation Procedure.

4.11 The Supplier has no right of set-off, counterclaim, discount or abatement unless they are ordered to do so by a court.

5. The buyer's obligations to the supplier

5.1 If Supplier Non-Performance arises from an Authority Cause:

- (a) neither CCS or the Buyer can terminate a Contract under Clause 10.4.1;
- (b) the Supplier is entitled to reasonable and proven additional expenses and to relief from liability and Deduction under this Contract;
- (c) the Supplier is entitled to additional time needed to make the Delivery; and
- (d) the Supplier cannot suspend the ongoing supply of Deliverables.

5.2 Clause 5.1 only applies if the Supplier:

- (a) gives notice to the Party responsible for the Authority Cause within 10 Working Days of becoming aware;
- (b) demonstrates that the Supplier Non-Performance would not have occurred but for the Authority

Cause; and

(c) mitigated the impact of the Authority Cause.

6. Record keeping and reporting

- 6.1 The Supplier must attend Progress Meetings with the Buyer and provide Progress Reports when specified in the Order Form.
- 6.2 The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Contract:
- (a) during the Contract Period;
 - (b) for 7 years after the End Date; and
 - (c) in accordance with UK GDPR,
- including but not limited to the records and accounts stated in the definition of Audit in Joint Schedule 1.
- 6.3 The Relevant Authority or an Auditor can Audit the Supplier.
- 6.4 During an Audit, the Supplier must:
- (a) allow the Relevant Authority or any Auditor access to their premises to verify all contract accounts and records of everything to do with the Contract and provide copies for an Audit; and
 - (b) provide information to the Relevant Authority or to the Auditor and reasonable co-operation at their request.
- 6.5 Where the Audit of the Supplier is carried out by an Auditor, the Auditor shall be entitled to share any information obtained during the Audit with the Relevant Authority.
- 6.6 If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:
- (a) tell the Relevant Authority and give reasons;
 - (b) propose corrective action; and
 - (c) provide a deadline for completing the corrective action.
- 6.7 The Supplier must provide CCS with a Self Audit Certificate supported by an audit report at the end of each Contract Year. The report must contain:
- (a) the methodology of the review;
 - (b) the sampling techniques applied;
 - (c) details of any issues; and
 - (d) any remedial action taken.
- 6.8 The Self Audit Certificate must be completed and signed by an auditor or senior member of the Supplier's management team that is qualified in either a relevant audit or financial discipline.

7. Supplier staff

- 7.1 The Supplier Staff involved in the performance of each Contract must:
- (a) be appropriately trained and qualified;
 - (b) be vetted using Good Industry Practice and the Security Policy; and
 - (c) comply with all conduct requirements when on the Buyer's Premises.
- 7.2 Where a Buyer decides one of the Supplier's Staff is not suitable to work on a contract, the Supplier must replace them with a suitably qualified alternative.
- 7.3 If requested, the Supplier must replace any person whose acts or omissions have caused the Supplier to breach Clause 27.
- 7.4 The Supplier must provide a list of Supplier Staff needing to access the Buyer's Premises and say why access is required.
- 7.5 The Supplier indemnifies CCS and the Buyer against all claims brought by any person employed by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.

8. Rights and protection

- 8.1 The Supplier warrants and represents that:
- (a) it has full capacity and authority to enter into and to perform each Contract;
 - (b) each Contract is executed by its authorised representative;
 - (c) it is a legally valid and existing organisation incorporated in the place it was formed;
 - (d) there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its Affiliates that might affect its ability to perform each Contract;
 - (e) it maintains all necessary rights, authorisations, licences and consents to perform its obligations under each Contract;
 - (f) it does not have any contractual obligations which are likely to have a material adverse effect on its ability to perform each Contract;
 - (g) it is not impacted by an Insolvency Event; and
 - (h) it will comply with each Call-Off Contract.
- 8.2 The warranties and representations in Clauses 2.10 and 8.1 are repeated each time the Supplier provides Deliverables under the Contract.
- 8.3 The Supplier indemnifies both CCS and every Buyer against each of the following:
- (a) wilful misconduct of the Supplier, Subcontractor and Supplier Staff that impacts the Contract; and
 - (b) non-payment by the Supplier of any Tax or National Insurance.

- 8.4 All claims indemnified under this Contract must use Clause 26.
- 8.5 The description of any provision of this Contract as a warranty does not prevent CCS or a Buyer from exercising any termination right that it may have for breach of that clause by the Supplier.
- 8.6 If the Supplier becomes aware of a representation or warranty that becomes untrue or misleading, it must immediately notify CCS and every Buyer.
- 8.7 All third party warranties and indemnities covering the Deliverables must be assigned for the Buyer's benefit by the Supplier.

9. Intellectual Property Rights (IPRs)

- 9.1 Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable worldwide licence to use, change and sub-license the Supplier's Existing IPR to enable it to both:
- (a) receive and use the Deliverables; and
 - (b) make use of the deliverables provided by a Replacement Supplier.
- 9.2 Any New IPR created under a Contract is owned by the Buyer. The Buyer gives the Supplier a licence to use any Existing IPRs and New IPRs for the purpose of fulfilling its obligations during the Contract Period.
- 9.3 Where a Party acquires ownership of IPRs incorrectly under this Contract it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.
- 9.4 Neither Party has the right to use the other Party's IPRs, including any use of the other Party's names, logos or trademarks, except as provided in Clause 9 or otherwise agreed in writing.
- 9.5 If there is an IPR Claim, the Supplier indemnifies CCS and each Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result.
- 9.6 If an IPR Claim is made or anticipated the Supplier must at its own expense and the Buyer's sole option, either:
- (a) obtain for CCS and the Buyer the rights in Clause 9.1 and 9.2 without infringing any third party IPR; or
 - (b) replace or modify the relevant item with substitutes that do not infringe IPR without adversely affecting the functionality or performance of the Deliverables.
- 9.7 In spite of any other provisions of a Contract and for the avoidance of doubt, award of a Contract by the Buyer and placement of any contract task under it does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977 or Section 12 of the Registered Designs Act 1949. The Supplier acknowledges that any authorisation by the Buyer under its statutory powers must be expressly provided in writing, with reference to the acts authorised and the specific IPR involved.

10. Ending the contract or any subcontract

10.1 Contract Period

10.1.1 The Contract takes effect on the Start Date and ends on the End Date or earlier if required by Law.

10.1.2 The Relevant Authority can extend the Contract for the Extension Period by giving the Supplier no less than 3 Months' written notice before the Contract expires.

10.2 Ending the contract without a reason

10.2.1 CCS has the right to terminate the Framework Contract at any time without reason by giving the Supplier at least 30 days' notice.

10.2.2 Each Buyer has the right to terminate their Call-Off Contract at any time without reason by giving the Supplier not less than 90 days' written notice.

10.3 Rectification plan process

10.3.1 If there is a Default, the Relevant Authority may, without limiting its other rights, request that the Supplier provide a Rectification Plan, within 10 working days .

10.3.2 When the Relevant Authority receives a requested Rectification Plan it can either:

- (a) reject the Rectification Plan or revised Rectification Plan, giving reasons; or
- (b) accept the Rectification Plan or revised Rectification Plan (without limiting its rights) and the Supplier must immediately start work on the actions in the Rectification Plan at its own cost, unless agreed otherwise by the Parties.

10.3.3 Where the Rectification Plan or revised Rectification Plan is rejected, the Relevant Authority:

- (a) must give reasonable grounds for its decision; and
- (b) may request that the Supplier provides a revised Rectification Plan within 5 Working Days.

10.3.4 If the Relevant Authority rejects any Rectification Plan, including any revised Rectification Plan, the Relevant Authority does not have to request a revised Rectification Plan before exercising its right to terminate its Contract under Clause 10.4.3(a).

10.4 When CCS or the buyer can end a contract

10.4.1 If any of the following events happen, the Relevant Authority has the right to immediately terminate its Contract by issuing a Termination Notice to the Supplier:

- (a) there is a Supplier Insolvency Event;
- (b) there is a Default that is not corrected in line with an accepted Rectification Plan;
- (c) the Supplier does not provide a Rectification Plan within 10 days of the request;
- (d) there is any material Default of the Contract;
- (e) there is any material Default of any Joint Controller Agreement relating to any Contract;

Core Terms

- (f) there is a Default of Clauses 2.10, 9, 14, 15, 27, 32 or Framework Schedule 9 (Cyber Essentials) (where applicable) relating to any Contract;
- (g) there is a consistent repeated failure to meet the Performance Indicators in Framework Schedule 4 (Framework Management);
- (h) there is a Change of Control of the Supplier which is not pre-approved by the Relevant Authority in writing;
- (i) if the Relevant Authority discovers that the Supplier was in one of the situations in 57 (1) or 57(2) of the Regulations at the time the Contract was awarded; or
- (j) the Supplier or its Affiliates embarrass or bring CCS or the Buyer into disrepute or diminish the public trust in them.

10.4.2 CCS may terminate the Framework Contract if a Buyer terminates a Call-Off Contract for any of the reasons listed in Clause 10.4.1.

10.4.3 If any of the following non-fault based events happen, the Relevant Authority has the right to immediately terminate its Contract by issuing a Termination Notice to the Supplier:

- (a) the Relevant Authority rejects a Rectification Plan;
- (b) there is a Variation which cannot be agreed using Clause 24 (Changing the contract) or resolved using Clause 34 (Resolving disputes);
- (c) if there is a declaration of ineffectiveness in respect of any Variation; or
- (d) the events in 73 (1) (a) of the Regulations happen.

10.5 When the supplier can end the contract

The Supplier can issue a Reminder Notice if the Buyer does not pay an undisputed invoice on time. The Supplier can terminate a Call-Off Contract if the Buyer fails to pay an undisputed invoiced sum due and worth over 10% of the annual Contract Value within 30 days of the date of the Reminder Notice.

10.6 What happens if the contract ends

10.6.1 Where a Party terminates a Contract under any of Clauses 10.2.1, 10.2.2, 10.4.1, 10.4.2, 10.4.3, 10.5 or 20.2 or a Contract expires all of the following apply:

- (a) The Buyer's payment obligations under the terminated Contract stop immediately.
- (b) Accumulated rights of the Parties are not affected.
- (c) The Supplier must promptly repay to the Buyer any and all Charges the Buyer has paid in advance in respect of Deliverables not provided by the Supplier as at the End Date.
- (d) The Supplier must promptly delete or return the Government Data except where required to retain copies by Law.
- (e) The Supplier must promptly return any of CCS or the Buyer's property provided under the terminated Contract.
- (f) The Supplier must, at no cost to CCS or the Buyer, co-operate fully in the handover and re-procurement (including to a Replacement Supplier).

10.6.2 In addition to the consequences of termination listed in Clause 10.6.1, where the Relevant Authority

Core Terms

terminates a Contract under Clause 10.4.1 the Supplier is also responsible for the Relevant Authority's reasonable costs of procuring Replacement Deliverables for the rest of the Contract Period.

10.6.3 In addition to the consequences of termination listed in Clause 10.6.1, if either the Relevant Authority terminates a Contract under Clause 10.2.1 or 10.2.2 or a Supplier terminates a Call-Off Contract under Clause 10.5:

- (a) the Buyer must promptly pay all outstanding Charges incurred to the Supplier; and
- (b) the Buyer must pay the Supplier reasonable committed and unavoidable Losses as long as the Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Contract had not been terminated.

10.6.4 In addition to the consequences of termination listed in Clause 10.6.1, where a Party terminates under Clause 20.2 each Party must cover its own Losses.

10.6.5 The following Clauses survive the termination or expiry of each Contract: 3.2.10, 4.2, 6, 7.5, 9, 11, 12.2, 14, 15, 16, 17, 18, 31.3, 34, 35 and any Clauses and Schedules which are expressly or by implication intended to continue.

10.7 Partially ending and suspending the contract

10.7.1 Where CCS has the right to terminate the Framework Contract it can suspend the Supplier's ability to accept Orders (for any period) and the Supplier cannot enter into any new Call-Off Contracts during this period. If this happens, the Supplier must still meet its obligations under any existing Call-Off Contracts that have already been signed.

10.7.2 Where CCS has the right to terminate a Framework Contract it is entitled to terminate all or part of it.

10.7.3 Where the Buyer has the right to terminate a Call-Off Contract it can terminate or suspend (for any period), all or part of it. If the Buyer suspends a Contract it can provide the Deliverables itself or buy them from a third party.

10.7.4 The Relevant Authority can only partially terminate or suspend a Contract if the remaining parts of that Contract can still be used to effectively deliver the intended purpose.

10.7.5 The Parties must agree any necessary Variation required by Clause 10.7 using the Variation Procedure, but the Supplier may not either:

- (a) reject the Variation; or
- (b) increase the Charges, except where the right to partial termination is under Clause 10.2.

10.7.6 The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under Clause 10.7.

10.8 When subcontracts can be ended

At the Buyer's request, the Supplier must terminate any Subcontracts in any of the following events:

- (a) there is a Change of Control of a Subcontractor which is not pre-approved by the Relevant Authority in writing;
- (b) the acts or omissions of the Subcontractor have caused or materially contributed to a right of termination under Clause 10.4; or
- (c) a Subcontractor or its Affiliates embarrasses or brings into disrepute or diminishes the public trust in the Relevant Authority.

11. How much you can be held responsible for

- 11.1 Each Party's total aggregate liability in each Contract Year under this Framework Contract (whether in tort, contract or otherwise) is no more than £1,000,000.
- 11.2 Each Party's total aggregate liability in each Contract Year under each Call-Off Contract (whether in tort, contract or otherwise) is no more than the greater of £5 million or 150% of the Estimated Yearly Charges unless specified in the Call-Off Order Form.
- 11.3 No Party is liable to the other for:
- (a) any indirect Losses; or
 - (b) Loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect).
- 11.4 In spite of Clause 11.1 and 11.2, neither Party limits or excludes any of the following:
- (a) its liability for death or personal injury caused by its negligence, or that of its employees, agents or Subcontractors;
 - (b) its liability for bribery or fraud or fraudulent misrepresentation by it or its employees;
 - (c) any liability that cannot be excluded or limited by Law;
 - (d) its obligation to pay the required Management Charge or Default Management Charge.
- 11.5 In spite of Clauses 11.1 and 11.2, the Supplier does not limit or exclude its liability for any indemnity given under Clauses 7.5, 8.3(b), 9.5, 31.3 or Call-Off Schedule 2 (Staff Transfer) of a Contract.
- 11.6 In spite of Clauses 11.1, 11.2 but subject to Clauses 11.3 and 11.4, the Supplier's aggregate liability in each and any Contract Year under each Contract under Clause 14.8 shall in no event exceed the Data Protection Liability Cap.
- 11.7 Each Party must use all reasonable endeavours to mitigate any Loss or damage which it suffers under or in connection with each Contract, including any indemnities.
- 11.8 When calculating the Supplier's liability under Clause 11.1 or 11.2 the following items will not be taken into consideration:
- (a) Deductions; and

(b) any items specified in Clauses 11.5 or 11.6.

11.9 If more than one Supplier is party to a Contract, each Supplier Party is jointly and severally liable for their obligations under that Contract.

12. Obeying the law

12.1 The Supplier must use reasonable endeavours to comply with the provisions of Joint Schedule 5 (Corporate Social Responsibility).

12.2 To the extent that it arises as a result of a Default by the Supplier, the Supplier indemnifies the Relevant Authority against any fine or penalty incurred by the Relevant Authority pursuant to Law and any costs incurred by the Relevant Authority in defending any proceedings which result in such fine or penalty.

12.3 The Supplier must appoint a Compliance Officer who must be responsible for ensuring that the Supplier complies with Law, Clause 12.1 and Clauses 27 to 32.

13. Insurance

The Supplier must, at its own cost, obtain and maintain the Required Insurances in Joint Schedule 3 (Insurance Requirements) and any Additional Insurances in the Order Form.

14. Data protection

14.1 The Supplier must process Personal Data and ensure that Supplier Staff process Personal Data only in accordance with Joint Schedule 11 (Processing Data).

14.2 The Supplier must not remove any ownership or security notices in or relating to the Government Data.

14.3 The Supplier must make accessible back-ups of all Government Data, stored in an agreed off-site location and send the Buyer copies every 6 Months.

14.4 The Supplier must ensure that any Supplier system holding any Government Data, including back-up data, is a secure system that complies with the Security Policy and any applicable Security Management Plan.

14.5 If at any time the Supplier suspects or has reason to believe that the Government Data provided under a Contract is corrupted, lost or sufficiently degraded, then the Supplier must notify the Relevant Authority and immediately suggest remedial action.

14.6 If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Relevant Authority may either or both:

- (a) tell the Supplier to restore or get restored Government Data as soon as practical but no later than 5 Working Days from the date that the Relevant Authority receives notice, or the Supplier finds out about the issue, whichever is earlier; and/or
- (b) restore the Government Data itself or using a third party.

14.7 The Supplier must pay each Party's reasonable costs of complying with Clause 14.6 unless CCS or the Buyer is at fault.

14.8 The Supplier:

- (a) must provide the Relevant Authority with all Government Data in an agreed open format within 10 Working Days of a written request;
- (b) must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading;
- (c) must securely destroy all Storage Media that has held Government Data at the end of life of that media using Good Industry Practice;
- (d) securely erase all Government Data and any copies it holds when asked to do so by CCS or the Buyer unless required by Law to retain it; and
- (e) indemnifies CCS and each Buyer against any and all Losses incurred if the Supplier breaches Clause 14 and any Data Protection Legislation.

15. What you must keep confidential

15.1 Each Party must:

- (a) keep all Confidential Information it receives confidential and secure;
- (b) except as expressly set out in the Contract at Clauses 15.2 to 15.4 or elsewhere in the Contract, not disclose, use or exploit the Disclosing Party's Confidential Information without the Disclosing Party's prior written consent; and
- (c) immediately notify the Disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information.

15.2 In spite of Clause 15.1, a Party may disclose Confidential Information which it receives from the Disclosing Party in any of the following instances:

- (a) where disclosure is required by applicable Law or by a court with the relevant jurisdiction if, to the extent not prohibited by Law, the Recipient Party notifies the Disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure;
- (b) if the Recipient Party already had the information without obligation of confidentiality before it was disclosed by the Disclosing Party;
- (c) if the information was given to it by a third party without obligation of confidentiality;
- (d) if the information was in the public domain at the time of the disclosure;
- (e) if the information was independently developed without access to the Disclosing Party's Confidential Information;
- (f) on a confidential basis, to its auditors;
- (g) on a confidential basis, to its professional advisers on a need-to-know basis; or
- (h) to the Serious Fraud Office where the Recipient Party has reasonable grounds to believe that the Disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010.

Core Terms

- 15.3 In spite of Clause 15.1, the Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Contract. The Supplier Staff must enter into a direct confidentiality agreement with the Relevant Authority at its request.
- 15.4 In spite of Clause 15.1, CCS or the Buyer may disclose Confidential Information in any of the following cases:
- (a) on a confidential basis to the employees, agents, consultants and contractors of CCS or the Buyer;
 - (b) on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company that CCS or the Buyer transfers or proposes to transfer all or any part of its business to;
 - (c) if CCS or the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions;
 - (d) where requested by Parliament; or
 - (e) under Clauses 4.7 and 16.
- 15.5 For the purposes of Clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in Clause 15.
- 15.6 Transparency Information is not Confidential Information.
- 15.7 The Supplier must not make any press announcement or publicise the Contracts or any part of them in any way, without the prior written consent of the Relevant Authority and must take all reasonable steps to ensure that Supplier Staff do not either.

16. When you can share information

- 16.1 The Supplier must tell the Relevant Authority within 48 hours if it receives a Request For Information.
- 16.2 Within five (5) Working Days of the Buyer's request the Supplier must give CCS and each Buyer full co-operation and information needed so the Buyer can:
- (a) publish the Transparency Information;
 - (b) comply with any Freedom of Information Act (FOIA) request; and/or
 - (c) comply with any Environmental Information Regulations (EIR) request.
- 16.3 The Relevant Authority may talk to the Supplier to help it decide whether to publish information under Clause 16. However, the extent, content and format of the disclosure is the Relevant Authority's decision in its absolute discretion.

17. Invalid parts of the contract

If any part of a Contract is prohibited by Law or judged by a court to be unlawful, void or unenforceable, it must be read as if it was removed from that Contract as much as required and rendered ineffective as far as

possible without affecting the rest of the Contract, whether it is valid or enforceable.

18. No other terms apply

The provisions incorporated into each Contract are the entire agreement between the Parties. The Contract replaces all previous statements, agreements and any course of dealings made between the Parties, whether written or oral, in relation to its subject matter. No other provisions apply.

19. Other people's rights in a contract

No third parties may use the Contracts (Rights of Third Parties) Act 1999 (CRTPA) to enforce any term of the Contract unless stated (referring to CRTPA) in the Contract. This does not affect third party rights and remedies that exist independently from CRTPA.

20. Circumstances beyond your control

20.1 Any Party affected by a Force Majeure Event is excused from performing its obligations under a Contract while the inability to perform continues, if it both:

- (a) provides a Force Majeure Notice to the other Party; and
- (b) uses all reasonable measures practical to reduce the impact of the Force Majeure Event.

20.2 Either Party can partially or fully terminate the affected Contract if the provision of the Deliverables is materially affected by a Force Majeure Event which lasts for 90 days continuously.

21. Relationships created by the contract

No Contract creates a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

22. Giving up contract rights

A partial or full waiver or relaxation of the terms of a Contract is only valid if it is stated to be a waiver in writing to the other Party.

23. Transferring responsibilities

- 23.1 The Supplier cannot assign, novate or transfer a Contract or any part of a Contract without the Relevant Authority's written consent.
- 23.2 The Relevant Authority can assign, novate or transfer its Contract or any part of it to any Central Government Body, public or private sector body which performs the functions of the Relevant Authority.
- 23.3 When CCS or the Buyer uses its rights under Clause 23.2 the Supplier must enter into a novation agreement in the form that CCS or the Buyer specifies.
- 23.4 The Supplier can terminate a Contract novated under Clause 23.2 to a private sector body that is experiencing an Insolvency Event.

23.5 The Supplier remains responsible for all acts and omissions of the Supplier Staff as if they were its own.

23.6 If CCS or the Buyer asks the Supplier for details about Subcontractors, the Supplier must provide details of Subcontractors at all levels of the supply chain including:

- (a) their name;
- (b) the scope of their appointment; and
- (c) the duration of their appointment.

24. Changing the contract

24.1 Either Party can request a Variation which is only effective if agreed in writing and signed by both Parties.

24.2 The Supplier must provide an Impact Assessment either:

- (a) with the Variation Form, where the Supplier requests the Variation; or
- (b) within the time limits included in a Variation Form requested by CCS or the Buyer.

24.3 If the Variation cannot be agreed or resolved by the Parties, CCS or the Buyer can either:

- (a) agree that the Contract continues without the Variation; or
- (b) terminate the affected Contract, unless in the case of a Call-Off Contract, the Supplier has already provided part or all of the provision of the Deliverables, or where the Supplier can show evidence of substantial work being carried out to provide them; or
- (c) refer the Dispute to be resolved using Clause 34 (Resolving Disputes).

24.4 CCS and the Buyer are not required to accept a Variation request made by the Supplier.

24.5 If there is a General Change in Law, the Supplier must bear the risk of the change and is not entitled to ask for an increase to the Framework Prices or the Charges.

24.6 If there is a Specific Change in Law or one is likely to happen during the Contract Period the Supplier must give CCS and the Buyer notice of the likely effects of the changes as soon as reasonably practical. They must also say if they think any Variation is needed either to the Deliverables, Framework Prices or a Contract and provide evidence:

- (a) that the Supplier has kept costs as low as possible, including in Subcontractor costs; and
- (b) of how it has affected the Supplier's costs.

24.7 Any change in the Framework Prices or relief from the Supplier's obligations because of a Specific Change in Law must be implemented using Clauses 24.1 to 24.4.

24.8 For 101(5) of the Regulations, if the Court declares any Variation ineffective, the Parties agree that their

mutual rights and obligations will be regulated by the terms of the Contract as they existed immediately prior to that Variation and as if the Parties had never entered into that Variation.

25. How to communicate about the contract

- 25.1 All notices under the Contract must be in writing and are considered effective on the Working Day of delivery as long as they are delivered before 5:00pm on a Working Day. Otherwise the notice is effective on the next Working Day. An email is effective at 9:00am on the first Working Day after sending unless an error message is received.
- 25.2 Notices to CCS must be sent to the CCS Authorised Representative's address or email address in the Framework Award Form.
- 25.3 Notices to the Buyer must be sent to the Buyer Authorised Representative's address or email address in the Order Form.
- 25.4 This Clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

26. Dealing with claims

- 26.1 If a Beneficiary is notified of a Claim then it must notify the Indemnifier as soon as reasonably practical and no later than 10 Working Days.
- 26.2 At the Indemnifier's cost the Beneficiary must both:
 - (a) allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim; and
 - (b) give the Indemnifier reasonable assistance with the claim if requested.
- 26.3 The Beneficiary must not make admissions about the Claim without the prior written consent of the Indemnifier which can not be unreasonably withheld or delayed.
- 26.4 The Indemnifier must consider and defend the Claim diligently using competent legal advisors and in a way that does not damage the Beneficiary's reputation.
- 26.5 The Indemnifier must not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay.
- 26.6 Each Beneficiary must take all reasonable steps to minimise and mitigate any losses that it suffers because of the Claim.
- 26.7 If the Indemnifier pays the Beneficiary money under an indemnity and the Beneficiary later recovers money which is directly related to the Claim, the Beneficiary must immediately repay the Indemnifier the lesser of either:
 - (a) the sum recovered minus any legitimate amount spent by the Beneficiary when recovering this money; or

- (b) the amount the Indemnifier paid the Beneficiary for the Claim.

27. Preventing fraud, bribery and corruption

27.1 The Supplier must not during any Contract Period:

- (a) commit a Prohibited Act or any other criminal offence in the Regulations 57(1) and 57(2); or
- (b) do or allow anything which would cause CCS or the Buyer, including any of their employees, consultants, contractors, Subcontractors or agents to breach any of the Relevant Requirements or incur any liability under them.

27.2 The Supplier must during the Contract Period:

- (a) create, maintain and enforce adequate policies and procedures to ensure it complies with the Relevant Requirements to prevent a Prohibited Act and require its Subcontractors to do the same;
- (b) keep full records to show it has complied with its obligations under Clause 27 and give copies to CCS or the Buyer on request; and
- (c) if required by the Relevant Authority, within 20 Working Days of the Start Date of the relevant Contract, and then annually, certify in writing to the Relevant Authority, that they have complied with Clause 27, including compliance of Supplier Staff, and provide reasonable supporting evidence of this on request, including its policies and procedures.

27.3 The Supplier must immediately notify CCS and the Buyer if it becomes aware of any breach of Clauses 27.1 or 27.2 or has any reason to think that it, or any of the Supplier Staff, has either:

- (a) been investigated or prosecuted for an alleged Prohibited Act;
- (b) been debarred, suspended, proposed for suspension or debarment, or is otherwise ineligible to take part in procurement programmes or contracts because of a Prohibited Act by any government department or agency;
- (c) received a request or demand for any undue financial or other advantage of any kind related to a Contract; or
- (d) suspected that any person or Party directly or indirectly related to a Contract has committed or attempted to commit a Prohibited Act.

27.4 If the Supplier notifies CCS or the Buyer as required by Clause 27.3, the Supplier must respond promptly to their further enquiries, co-operate with any investigation and allow the Audit of any books, records and relevant documentation.

27.5 In any notice the Supplier gives under Clause 27.3 it must specify the:

- (a) Prohibited Act;
- (b) identity of the Party who it thinks has committed the Prohibited Act; and
- (c) action it has decided to take.

28. Equality, diversity and human rights

28.1 The Supplier must follow all applicable equality Law when they perform their obligations under the Contract, including:

- (a) protections against discrimination on the grounds of race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise; and
- (b) any other requirements and instructions which CCS or the Buyer reasonably imposes related to equality Law.

28.2 The Supplier must take all necessary steps, and inform CCS or the Buyer of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on a Contract.

29. Health and safety

29.1 The Supplier must perform its obligations meeting the requirements of:

- (a) all applicable Law regarding health and safety; and
- (b) the Buyer's current health and safety policy while at the Buyer's Premises, as provided to the Supplier.

29.2 The Supplier and the Buyer must as soon as possible notify the other of any health and safety incidents or material hazards they are aware of at the Buyer Premises that relate to the performance of a Contract.

30. Environment

30.1 When working on Site the Supplier must perform its obligations under the Buyer's current Environmental Policy, which the Buyer must provide.

30.2 The Supplier must ensure that Supplier Staff are aware of the Buyer's Environmental Policy.

31. Tax

31.1 The Supplier must not breach any Tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines. CCS and the Buyer cannot terminate a Contract where the Supplier has not paid a minor Tax or social security contribution.

31.2 Where the Charges payable under a Contract with the Buyer are or are likely to exceed £5 million at any point during the relevant Contract Period, and an Occasion of Tax Non-Compliance occurs, the Supplier must notify CCS and the Buyer of it within 5 Working Days including:

- (a) the steps that the Supplier is taking to address the Occasion of Tax Non-Compliance and any mitigating factors that it considers relevant; and
- (b) other information relating to the Occasion of Tax Non-Compliance that CCS and the Buyer may

reasonably need.

31.3 Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance contributions in the UK relating to payment received under a Call-Off Contract, the Supplier must both:

- (a) comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, the Social Security Contributions and Benefits Act 1992 (including IR35) and National Insurance contributions; and
- (b) indemnify the Buyer against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Contract Period in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff.

31.4 If any of the Supplier Staff are Workers who receive payment relating to the Deliverables, then the Supplier must ensure that its contract with the Worker contains the following requirements:

- (a) the Buyer may, at any time during the Contract Period, request that the Worker provides information which demonstrates they comply with Clause 31.3, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding;
- (b) the Worker's contract may be terminated at the Buyer's request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer;
- (c) the Worker's contract may be terminated at the Buyer's request if the Worker provides information which the Buyer considers is not good enough to demonstrate how it complies with Clause 31.3 or confirms that the Worker is not complying with those requirements; and
- (d) the Buyer may supply any information they receive from the Worker to HMRC for revenue collection and management.

32. Conflict of interest

32.1 The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual or potential Conflict of Interest.

32.2 The Supplier must promptly notify and provide details to CCS and each Buyer if a Conflict of Interest happens or is expected to happen.

32.3 CCS and each Buyer can terminate its Contract immediately by giving notice in writing to the Supplier or take any steps it thinks are necessary where there is or may be an actual or potential Conflict of Interest.

33. Reporting a breach of the contract

33.1 As soon as it is aware of it the Supplier and Supplier Staff must report to CCS or the Buyer any actual or suspected breach of:

- (a) Law;
- (b) Clause 12.1; or

(c) Clauses 27 to 32.

33.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in Clause 33.1 to the Buyer or a Prescribed Person.

34. Resolving disputes

34.1 If there is a Dispute, the senior representatives of the Parties who have authority to settle the Dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the Dispute.

34.2 If the Dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution (CEDR) Model Mediation Procedure current at the time of the Dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the Dispute, the Dispute must be resolved using Clauses 34.3 to 34.5.

34.3 Unless the Relevant Authority refers the Dispute to arbitration using Clause 34.4, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:

- (a) determine the Dispute;
- (b) grant interim remedies; and/or
- (c) grant any other provisional or protective relief.

34.4 The Supplier agrees that the Relevant Authority has the exclusive right to refer any Dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the Dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

34.5 The Relevant Authority has the right to refer a Dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under Clause 34.3, unless the Relevant Authority has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under Clause 34.4.

34.6 The Supplier cannot suspend the performance of a Contract during any Dispute.

35. Which law applies

This Contract and any Disputes arising out of, or connected to it, are governed by English law.

Framework Special Terms

Framework Special Terms

Below are the Framework Special Terms specified in the Framework Award Form and incorporated into the Framework Contract:

Special Term 1	A new Clause 2.11 shall be added to the Core Terms: “The Supplier shall operate the Catalogue in accordance with Framework Schedule 1 (Specification).”
Special Term 2	Clause 3.2.11 of the Core Terms shall be deleted and replaced with the following: “Not used.”
Special Term 3	Clause 3.2.2 of the Core Terms shall be deleted and replaced with the following: “Not used.”
Special Term 4	Clause 7.4 of the Core Terms shall be deleted and replaced with the following: “If requested, the Supplier will provide a list of Supplier Staff needing access to the Buyer's Premises and say why access is required”
Special Term 5	Clause 8.7 of the Core Terms shall be deleted and replaced with the following: “The Supplier shall assign to the Buyer, or if it is unable to do so, shall (to the extent it is legally able to do so) hold on trust for the sole benefit of the Buyer, those warranties and indemnities provided by third parties that are specifically associated with and particular to the Deliverables provided to the Buyer. Where any such warranties are held on trust, the Supplier shall enforce such warranties as required by the Buyer on the Buyer's behalf in order to provide the Services and shall do so in accordance with any reasonable directions that the Buyer may notify from time to time to the Supplier.”
Special Term 6	Core Terms Clause 11.2 – amend “£5 million” to “£1 million”
Special Term 7	Clause 14.1 of the Core Terms shall be deleted and replaced with the following: “The Parties acknowledge that for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor unless otherwise specified in Joint Schedule 11. The Supplier must process Personal Data and ensure that Supplier Staff process Personal Data only in

	accordance with Joint Schedule 11 (Processing Data)."
Special Term 8	<p>Core Terms Clause 24.2 – add the following additional text at the end of the Clause :</p> <p>"If the Supplier needs resources other than those ordinarily used in the provision of the Service in order to complete an Impact Assessment requested by the Buyer, the Supplier must tell the Buyer before beginning the Impact Assessment. If the Buyer wants the Impact Assessment to go ahead, the Buyer shall pay any reasonable costs incurred by the Supplier in producing the Impact Assessment. To be clear, the Supplier will not be able to recover costs incurred during the Impact Assessment that the Buyer didn't agree before the Impact Assessment began."</p>
Special Term 9	<p>Core Terms – add the following provision:</p> <p>"36. Telecoms Expense Management The Supplier shall provide without charge to a TEM Provider nominated by the Buyer the detailed invoice data for each Buyer in receipt of Deliverables in an Electronic Data Interchange (EDI) format at the same frequency as it is received by that Buyer, subject to the TEM Provider agreeing to enter into a direct confidentiality agreement with the Supplier on terms equivalent to the terms set out in Clause 15 (What you must keep Confidential)."</p>
Special Term 10	<p>Joint Schedule 5 – Corporate Social Responsibility</p> <p>The application of clause 3.1.8 within Joint Schedule 5 - Corporate Social Responsibility applies only in respect of Lot 1a</p>
Special Term 11	<p>Clause 10.2.2 of the Core Terms shall be deleted and replaced with the following:</p> <p>"Each Buyer has the right to terminate their Call-Off Contract at any time by giving the Supplier not less than the minimum period of notice specified in the Order Form or 90 days (whichever is greater)."</p>

Joint Schedule 1 (Definitions)

Crown Copyright 2018

Joint Schedule 1 (Definitions)

- 1.1 In each Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Joint 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 each 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 Central Government 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;
 - 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 each Contract are for ease of reference only and shall not affect the interpretation or construction of a Contract;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

1.3.12 where the Buyer is a Central Government Body it shall be treated as contracting with the Crown as a whole;

1.3.13 any reference in a Contract which immediately before Exit Day was 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 Exit 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 Exit Day as a reference to the UK institution, authority or body to which its functions were transferred; and

1.3.14 unless otherwise provided, references to "**Buyer**" shall be construed as including Exempt Buyers; and

1.3.15 unless otherwise provided, references to "**Call-Off Contract**" and "**Contract**" shall be construed as including Exempt Call-off Contracts.

1.4 In each Contract, unless the context otherwise requires, the following words shall have the following meanings:

Accounting Reference Date	means in each year the date to which the Supplier prepares its annual audited financial statements;
"Achieve"	in respect of a Test, to successfully pass such Test without any Test Issues and in respect of a Milestone, the issue of a Satisfaction Certificate in respect of that Milestone and " Achieved ", " Achieving " and " Achievement " shall be construed accordingly;
"Additional Insurances"	insurance requirements relating to a Call-Off Contract specified in the Order Form additional to those outlined in Joint Schedule 3 (Insurance Requirements);
"Admin Fee"	means the costs incurred by CCS in dealing with MI Failures calculated in accordance with the tariff of administration charges published by the CCS on: http://CCS.cabinetoffice.gov.uk/i-am-supplier/management-information/admin-fees ;
"Affected Party"	the Party seeking to claim relief in respect of a Force Majeure Event;
"Affiliates"	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;
"Annex"	extra information which supports a Schedule;
"Approval"	the prior written consent of the Buyer and " Approve " and " Approved " shall be construed accordingly;

Framework Ref: RM6116

Project Version: v1.0

Model Version: v3.10

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Audit"	<p>the Relevant Authority's right to:</p> <ul style="list-style-type: none"> a) verify the accuracy of the Charges and any other amounts payable by a Buyer under a Call-Off Contract (including proposed or actual variations to them in accordance with the Contract); b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Services; a) where the Relevant Authority is a Buyer, and the value of the relevant Call-Off Contract is greater than £3million, verify the Open Book Data; c) verify the Supplier's and each Subcontractor's compliance with the Contract and applicable Law; d) identify or investigate actual or suspected breach of Clauses 27 to 33 and/or Joint Schedule 5 (Corporate Social Responsibility), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Relevant Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations; e) identify or investigate any circumstances which may impact upon the financial stability of the Supplier, any Guarantor, and/or any Subcontractors or their ability to provide the Deliverables; f) obtain such information as is necessary to fulfil the Relevant Authority's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General; g) review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract; h) carry out the Relevant Authority's internal and statutory audits and to prepare, examine and/or certify the Relevant Authority's annual and interim reports and accounts; i) 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 Relevant Authority has used its resources; or j) verify the accuracy and completeness of any Management Information delivered or required by the Framework Contract;
"Auditor"	<p>means:</p> <ul style="list-style-type: none"> a) the Relevant Authority's internal and external auditors; b) the Relevant 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;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	e) any party formally appointed by the Relevant Authority to carry out audit or similar review functions; and f) successors or assigns of any of the above;
"Authority"	CCS and each Buyer;
"Authority Cause"	any breach of the obligations of the Relevant Authority or any other default, act, omission, negligence or statement of the Relevant Authority, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Relevant Authority is liable to the Supplier;
"BACS"	the Bankers' Automated Clearing Services, which is a scheme for the electronic processing of financial transactions within the United Kingdom;
"Beneficiary"	a Party having (or claiming to have) the benefit of an indemnity under this Contract;
"Buyer"	the relevant public sector purchaser identified as such in the Order Form;
"Buyer Assets"	the Buyer's infrastructure, data, software, materials, assets, equipment or other property owned by and/or licensed or leased to the Buyer and which is or may be used in connection with the provision of the Deliverables which remain the property of the Buyer throughout the term of the Contract;
"Buyer Authorised Representative"	the representative appointed by the Buyer from time to time in relation to the Call-Off Contract initially identified in the Order Form;
"Buyer Premises"	premises owned, controlled or occupied by the Buyer which are made available for use by the Supplier or its Subcontractors for the provision of the Deliverables (or any of them);
Buyer System	has the meaning given to it in Schedule 6 (ICT Services);
"Call-Off Contract"	the contract between the Buyer and the Supplier (entered into pursuant to the provisions of the Framework Contract), which consists of the terms set out and referred to in the Order Form;
"Call-Off Contract Period"	the Contract Period in respect of the Call-Off Contract;
"Call-Off Expiry Date"	the scheduled date of the end of a Call-Off Contract as stated in the Order Form;
"Call-Off Incorporated Terms"	the contractual terms applicable to the Call-Off Contract specified under the relevant heading in the Order Form;
"Call-Off Initial Period"	the Initial Period of a Call-Off Contract specified in the Order Form;
Call Off Optional Extension Period	such period or periods beyond which the Call-Off Initial Period may be extended up to a maximum of the number of years in total specified in the Order Form

Framework Ref: RM6116

Project Version: v1.0

Model Version: v3.10

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Call-Off Procedure"	the process for awarding a Call-Off Contract pursuant to Clause 2 (How the contract works) and Framework Schedule 7 (Call-Off Award Procedure);
"Call-Off Special Terms"	any additional terms and conditions specified in the Order Form incorporated into the applicable Call-Off Contract;
"Call-Off Start Date"	the date of start of a Call-Off Contract as stated in the Order Form;
"Call-Off Tender"	the tender submitted by the Supplier in response to the Buyer's Statement of Requirements following a Further Competition Procedure and set out at Call-Off Schedule 4 (Call-Off Tender);
Catalogue	the Supplier's catalogue of Deliverables available to Buyers to order without Further Competition;
Catalogue Publication Portal	the CCS online publication channel via which Buyers can view the Catalogue;
"CCS"	the Minister for the Cabinet Office as represented by Crown Commercial Service, which is an executive agency and operates as a trading fund of the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool L3 9PP;
"CCS Authorised Representative"	the representative appointed by CCS from time to time in relation to the Framework Contract initially identified in the Framework Award Form;
"Central Government Body"	<p>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:</p> <ul style="list-style-type: none"> 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;
"Change in Law"	any change in Law which impacts on the supply of the Deliverables and performance of the Contract which comes into force after the Start Date;
"Change of Control"	a change of control within the meaning of Section 450 of the Corporation Tax Act 2010;
"Charges"	the prices (exclusive of any applicable VAT), payable to the Supplier by the Buyer under the Call-Off Contract, as set out in the Order Form, for the full and proper performance by the Supplier of its obligations under the Call-Off Contract less any Deductions;
"Claim"	any claim which it appears that a Beneficiary is, or may become, entitled to indemnification under this Contract;
"Commercially Sensitive Information"	the Confidential Information listed in the Framework Award Form or Order Form (if any) comprising of commercially sensitive information relating to the Supplier, its IPR or its business or which the Supplier has indicated to

Framework Ref: RM6116

Project Version: v1.0

Model Version: v3.10

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss;
"Comparable Supply"	the supply of Deliverables to another Buyer of the Supplier that are the same or similar to the Deliverables;
"Compliance Officer"	the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;
"Confidential Information"	means any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, Know-How, personnel and suppliers of CCS, the Buyer or the Supplier, including IPRs, together with information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential;
"Conflict of Interest"	a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to CCS or any Buyer under a Contract, in the reasonable opinion of the Buyer or CCS;
"Contract"	either the Framework Contract or the Call-Off Contract, as the context requires;
"Contract Period"	the term of either a Framework Contract or Call-Off Contract on and from the earlier of the: a) applicable Start Date; or b) the Effective Date up to and including the applicable End Date;
"Contract Value"	the higher of the actual or expected total Charges paid or payable under a Contract where all obligations are met by the Supplier;
"Contract Year"	a consecutive period of twelve (12) Months commencing on the Start Date or each anniversary thereof;
"Control"	control in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and "Controlled" shall be construed accordingly;
"Controller"	has the meaning given to it in the UK GDPR;
Core Network	the provision of any shared central core network capability forming part of the overall Services delivered to the Buyer, which is not specific or exclusive to a specific Call-Off Contract, and excludes any configuration information specifically associated with a specific CallOff Contract;
"Core Terms"	CCS' terms and conditions for common goods and services which govern how Suppliers must interact with CCS and Buyers under Framework Contracts and Call-Off Contracts;
"Costs"	the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Deliverables:

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	<p>a) the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Work Day, of engaging the Supplier Staff, including:</p> <ul style="list-style-type: none"> i) base salary paid to the Supplier Staff; ii) employer's National Insurance contributions; iii) pension contributions; iv) car allowances; v) any other contractual employment benefits; vi) staff training; vii) work place accommodation; viii) work place IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and ix) reasonable recruitment costs, as agreed with the Buyer; <p>b) costs incurred in respect of Supplier Assets 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 Supplier Assets by the Supplier to the Buyer or (to the extent that risk and title in any Supplier Asset is not held by the Supplier) any cost actually incurred by the Supplier in respect of those Supplier Assets;</p> <p>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 provision of the Deliverables; and</p> <p>d) Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables;</p> <p>but excluding:</p> <ul style="list-style-type: none"> i) Overhead; ii) financing or similar costs; iii) maintenance and support costs to the extent that these relate to maintenance and/or support Deliverables provided beyond the Call-Off Contract Period whether in relation to Supplier Assets or otherwise; iv) taxation; v) fines and penalties; vi) amounts payable under Call-Off Schedule 16 (Benchmarking) where such Schedule is used; and vii) non-cash items (including depreciation, amortisation, impairments and movements in provisions);
"CRTPA"	the Contract Rights of Third Parties Act 1999;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Data Protection Impact Assessment"	an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data;
"Data Protection Legislation"	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy;
"Data Protection Liability Cap"	the amount specified in the Framework Award Form;
"Data Protection Officer"	has the meaning given to it in the UK GDPR;
"Data Subject"	has the meaning given to it in the UK GDPR;
"Data Subject Access Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
"Deductions"	all Service Credits, Delay Payments (if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under a Call-Off Contract;
"Default"	any breach of the obligations of the Supplier (including abandonment of a Contract in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of a Contract and in respect of which the Supplier is liable to the Relevant Authority;
"Default Management Charge"	has the meaning given to it in Paragraph 8.1.1 of Framework Schedule 5 (Management Charges and Information);
"Delay Payments"	the amounts (if any) payable by the Supplier to the Buyer in respect of a delay in respect of a Milestone as specified in the Implementation Plan;
"Deliverables"	Goods and/or Services that may be ordered under the Contract including the Documentation;
"Delivery"	delivery of the relevant Deliverable or Milestone in accordance with the terms of a Call-Off Contract as confirmed and accepted by the Buyer by the either (a) confirmation in writing to the Supplier; or (b) where Call-Off Schedule 13 (Implementation Plan and Testing) is used issue by the Buyer of a Satisfaction Certificate. "Deliver" and "Delivered" shall be construed accordingly;
Direct Award Criteria	the award criteria to be applied for the direct award of CallOff Contracts for Services set out in Framework Schedule 7 (Call-Off Award Procedure);
"Disclosing Party"	the Party directly or indirectly providing Confidential Information to the other Party in accordance with Clause 15 (What you must keep confidential);

Framework Ref: RM6116

Project Version: v1.0

Model Version: v3.10

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Dispute"	any claim, dispute or difference (whether contractual or non-contractual) arising out of or in connection with the Contract or in connection with the negotiation, existence, legal validity, enforceability or termination of the Contract, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts;
"Dispute Resolution Procedure"	the dispute resolution procedure set out in Clause 34 (Resolving disputes);
"Documentation"	descriptions of the Services and Service Levels, technical specifications, user manuals, training manuals, operating manuals, process definitions and procedures, system environment descriptions and all such other documentation (whether in hardcopy or electronic form) is required to be supplied by the Supplier to the Buyer under a Contract as: would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Buyer to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide the Deliverables is required by the Supplier in order to provide the Deliverables; and/or has been or shall be generated for the purpose of providing the Deliverables;
"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;
"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 Start Date;
"Effective Date"	the date on which the final Party has signed the Contract;
"EIR"	the Environmental Information Regulations 2004;
"Electronic Invoice"	an invoice which has been issued, transmitted and received in a structured electronic format which allows for its automatic and electronic processing and which complies with (a) the European standard and (b) any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870;
"Employment Regulations"	the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the European Council Directive 77/187/EEC;
"End Date"	the earlier of:

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	the Expiry Date (as extended by any Extension Period exercised by the Relevant Authority under Clause 10.1.2); or if a Contract is terminated before the date specified in (a) above, the date of termination of the Contract;
"Environmental Policy"	to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Buyer;
"Equality and Human Rights Commission"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
"Estimated Year 1 Charges"	the anticipated total Charges payable by the Buyer in the first Contract Year specified in the Order Form;

"Estimated Yearly Charges"	means for the purposes of calculating each Party's annual liability under clause 11.2 : i) in the first Contract Year, the Estimated Year 1 Charges; or ii) in the any subsequent Contract Years, the Charges paid or payable in the previous Call-off Contract Year; or iii) after the end of the Call-off Contract, the Charges paid or payable in the last Contract Year during the Call-off Contract Period;
"Exempt Buyer"	a public sector purchaser that is: a) eligible to use the Framework Contract; and b) is entering into an Exempt Call-off Contract that is not subject to (as applicable) any of: i) the Regulations; ii) the Concession Contracts Regulations 2016 (SI 2016/273); iii) the Utilities Contracts Regulations 2016 (SI 2016/274); iv) the Defence and Security Public Contracts Regulations 2011 (SI 2011/1848); v) the Remedies Directive (2007/66/EC); vi) Directive 2014/23/EU of the European Parliament and Council; vii) Directive 2014/24/EU of the European Parliament and Council; viii) Directive 2014/25/EU of the European Parliament and Council; or

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	ix) Directive 2009/81/EC of the European Parliament and Council;
"Exempt Call-off Contract"	the contract between the Exempt Buyer and the Supplier for Deliverables which consists of the terms set out and referred to in the Order Form incorporating and, where necessary, amending, refining or adding to the terms of the Framework Contract;
"Exempt Procurement Amendments"	any amendments, refinements or additions to any of the terms of the Framework Contract made through the Exempt Call-off Contract to reflect the specific needs of an Exempt Buyer to the extent permitted by and in accordance with any legal requirements applicable to that Exempt Buyer;
"Existing IPR"	any and all IPR that are owned by or licensed to either Party and which are or have been developed independently of the Contract (whether prior to the Start Date or otherwise);
"Exit Day"	shall have the meaning in the European Union (Withdrawal) Act 2018;
"Expiry Date"	the Framework Expiry Date or the Call-Off Expiry Date (as the context dictates);
"Extension Period"	the Framework Optional Extension Period or the Call-Off Optional Extension Period as the context dictates;
Financial Reports	<p>a report by the Supplier to the Buyer that:</p> <ul style="list-style-type: none"> a) provides a true and fair reflection of the Costs and Supplier Profit Margin forecast by the Supplier; b) provides a true and fair reflection of the costs and expenses to be incurred by Key Subcontractors (as requested by the Buyer); c) is in the same software package (Microsoft Excel or Microsoft Word), layout and format as the blank templates which have been issued by the Buyer to the Supplier on or before the Start Date for the purposes of the Contract; and <p>is certified by the Supplier's Chief Financial Officer or Director of Finance;</p>
"FOIA"	the Freedom of Information Act 2000 as amended from time to time 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 relevant Government department in relation to such legislation;
"Force Majeure Event"	any event outside the reasonable control of either Party affecting its performance of its obligations under the Contract arising from acts,

Framework Ref: RM6116

Project Version: v1.0

Model Version: v3.10

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	<p>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:</p> <ul style="list-style-type: none"> a) riots, civil commotion, war or armed conflict; b) acts of terrorism; c) acts of government, local government or regulatory bodies; d) fire, flood, storm or earthquake or other natural disaster, <p>but excluding any industrial dispute relating to the Supplier, the Supplier Staff or any other failure in the Supplier or the Subcontractor's supply chain;</p>
"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;
"Framework Award Form"	the document outlining the Framework Incorporated Terms and crucial information required for the Framework Contract, to be executed by the Supplier and CCS;
"Framework Contract"	the framework agreement established between CCS and the Supplier in accordance with Regulation 33 by the Framework Award Form for the provision of the Deliverables to Buyers by the Supplier pursuant to the notice published on the Find a Tender Service;
"Framework Contract Period"	the period from the Framework Start Date until the End Date of the Framework Contract;
"Framework Expiry Date"	the scheduled date of the end of the Framework Contract as stated in the Framework Award Form;
"Framework Incorporated Terms"	the contractual terms applicable to the Framework Contract specified in the Framework Award Form;
Framework Initial Period	the initial term of the Framework Contract as specified in the Framework Award Form;
"Framework Optional Extension Period"	such period or periods beyond which the Framework Contract Period may be extended as specified in the Framework Award Form;
"Framework Price(s)"	the price(s) applicable to the provision of the Deliverables set out in Framework Schedule 3 (Framework Prices);
"Framework Special Terms"	any additional terms and conditions specified in the Framework Award Form incorporated into the Framework Contract;
"Framework Start Date"	the date of start of the Framework Contract as stated in the Framework Award Form;
"Framework Tender Response"	the tender submitted by the Supplier to CCS and annexed to or referred to in Framework Schedule 2 (Framework Tender);
"Further Competition Procedure"	the further competition procedure described in Framework Schedule 7 (Call-Off Award Procedure);

Framework Ref: RM6116

Project Version: v1.0

Model Version: v3.10

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"UK GDPR"	the retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679);
"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 Tax or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
Gold Contract	a Call-Off Contract categorised as a Gold contract using the Cabinet Office Contract Tiering Tool;
"Goods"	goods made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form ;
"Good Industry Practice"	standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector;
"Government"	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 other bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"Government Data"	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, including any of the Authority's Confidential Information, and which: i) are supplied to the Supplier by or on behalf of the Authority; or ii) the Supplier is required to generate, process, store or transmit pursuant to a Contract;
"Guarantor"	the person (if any) who has entered into a guarantee in the form set out in Joint Schedule 8 (Guarantee) in relation to this Contract;
HM Government	Her Majesty's Government;
"Halifax Abuse Principle"	the principle explained in the CJEU Case C-255/02 Halifax and others;
Health and Social Care Network or HCSN	the government's network for health and social care, which helps all organisations involved in health and social care delivery to work together and interoperate; and as described at https://digital.nhs.uk/services/health-and-social-care-network ;
"HMRC"	Her Majesty's Revenue and Customs;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

ICT Environment	the ICT systems related to a Call-Off Contract described in Call-Off Schedule 6 (ICT Services);
"ICT Policy"	the Buyer's policy in respect of information and communications technology, referred to in the Order Form, which is in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Variation Procedure;
ICT Services	the ICT related Services to be delivered under a Call-Off Contract described in Call-Off Schedule 6 (ICT Services);
"Impact Assessment"	<p>an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including:</p> <ul style="list-style-type: none"> a) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract; b) details of the cost of implementing the proposed Variation; c) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the Framework Prices/Charges (as applicable), any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party; d) a timetable for the implementation, together with any proposals for the testing of the Variation; and e) such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request;
"Implementation Plan"	the plan for provision of the Deliverables set out in Call-Off Schedule 13 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer;
"Indemnifier"	a Party from whom an indemnity is sought under this Contract;
"Independent Control"	where a Controller has provided Personal Data to another Party which is not a Processor or a Joint Controller because the recipient itself determines the purposes and means of Processing but does so separately from the Controller providing it with Personal Data and "Independent Controller" shall be construed accordingly;
"Indexation"	the adjustment of an amount or sum in accordance with Framework Schedule 3 (Framework Prices) and the relevant Order Form;
"Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;
"Information Commissioner"	the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;
"Initial Period"	the initial term of a Contract specified in the Framework Award Form or the Order Form, as the context requires;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Insolvency Event"	<p>with respect to any person, means:</p> <p>(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:</p> <p>(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</p> <p>(ii) (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986;</p> <p>(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;</p> <p>(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;</p> <p>(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 14 days;</p> <p>(e) that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business;</p> <p>(f) where that person is a company, a LLP or a partnership:</p> <p>(i) a petition is presented (which is not dismissed within 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;</p> <p>(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;</p> <p>(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</p>
---------------------------	---

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	<p>(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</p> <p>(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;</p>
"Installation Works"	all works which the Supplier is to carry out at the beginning of the Call-Off Contract Period to install the Goods in accordance with the Call-Off Contract;
"Intellectual Property Rights" or "IPR"	<p>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 or business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information;</p> <p>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</p> <p>c) all other rights having equivalent or similar effect in any country or jurisdiction;</p>
"Invoicing Address"	the address to which the Supplier shall invoice the Buyer as specified in the Order Form;
"IPR Claim"	any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR, used to provide the Deliverables or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Relevant Authority in the fulfilment of its obligations under a Contract;
"IR35"	the off-payroll rules requiring individuals who work through their company pay the same income tax and National Insurance contributions as an employee which can be found online at: https://www.gov.uk/guidance/ir35-find-out-if-it-applies ;
ISO	International Organization for Standardization;
"Joint Controller Agreement"	the agreement (if any) entered into between the Relevant Authority and the Supplier substantially in the form set out in Annex 2 of Joint Schedule 11 (<i>Processing Data</i>);
"Joint Controllers"	where two or more Controllers jointly determine the purposes and means of Processing;
"Key Staff"	the individuals (if any) identified as such in the Order Form;
"Key Sub-Contract"	each Sub-Contract with a Key Subcontractor;
"Key Subcontractor"	any Subcontractor;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	<p>a) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or</p> <p>b) which, in the opinion of CCS or the Buyer performs (or would perform if appointed) a critical role in the provision of all or any part of the Deliverables; and/or</p> <p>c) 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 the Call-Off Contract,</p> <p>and the Supplier shall list all such Key Subcontractors in section 19 of the Framework Award Form and in the Key Subcontractor Section in Order Form;</p>
"Know-How"	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Deliverables but excluding know-how already in the other Party's possession before the applicable Start Date;
"Law"	any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply;
"Losses"	all losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and "Loss" shall be interpreted accordingly;
"Lots"	the number of lots specified in Framework Schedule 1 (Specification), if applicable;
"Management Charge"	the sum specified in the Framework Award Form payable by the Supplier to CCS in accordance with Framework Schedule 5 (Management Charges and Information);
"Management Information" or "MI"	the management information specified in Framework Schedule 5 (Management Charges and Information);
"MI Default"	means when two (2) MI Reports are not provided in any rolling six (6) month period
"MI Failure"	<p>means when an MI report:</p> <p>a) contains any material errors or material omissions or a missing mandatory field; or</p> <p>b) is submitted using an incorrect MI reporting Template; or</p> <p>c) is not submitted by the reporting date (including where a declaration of no business should have been filed);</p>

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"MI Report"	means a report containing Management Information submitted to the Authority in accordance with Framework Schedule 5 (Management Charges and Information);
"MI Reporting Template"	means the form of report set out in the Annex to Framework Schedule 5 (Management Charges and Information) setting out the information the Supplier is required to supply to the Authority;
"Milestone"	an event or task described in the Implementation Plan;
"Milestone Date"	the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved;
"Month"	a calendar month and "Monthly" shall be interpreted accordingly;
"National Insurance"	contributions required by the Social Security Contributions and Benefits Act 1992 and made in accordance with the Social Security (Contributions) Regulations 2001 (SI 2001/1004);
Nationally Critical Public Sector Domains	<p>domains where loss of access or an outage (for any reason) would cause immediate and extended outages of public-facing digital services, disrupting citizens' access to the services they depend on including benefits, and loss and disruption of all Government internal communications, including public servants accessing their own internal IT.</p> <p>There are a number of nationally critical domains within the UK, including but not limited to .gov.uk, .nhs.uk, gov.scot, gov.wales, .police.uk and .mod.uk.</p>
"New IPR"	<p>a) IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of a Contract and updates and amendments of these items including (but not limited to) database schema; and/or</p> <p>b) IPR in or arising as a result of the performance of the Supplier's obligations under a Contract and all updates and amendments to the same;</p> <p>but shall not include the Supplier's Existing IPR;</p>
"Occasion of Tax Non-Compliance"	<p>where:</p> <p>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:</p> <ol style="list-style-type: none"> 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 in any jurisdiction that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle; 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 in any jurisdiction; and/or

Framework Ref: RM6116

Project Version: v1.0

Model Version: v3.10

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	b) any Tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which 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 Start Date or to a civil penalty for fraud or evasion;
"Open Book Data "	<p>complete and accurate financial and non-financial information which is sufficient to enable the Buyer to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the Call-Off Contract, including details and all assumptions relating to:</p> <ul style="list-style-type: none"> a) the Supplier's Costs broken down against each Good and/or Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all Deliverables; b) operating expenditure relating to the provision of the Deliverables including an analysis showing: <ul style="list-style-type: none"> i) the unit costs and quantity of Goods and any other consumables and bought-in Deliverables; ii) staff costs broken down into the number and grade/role of all Supplier Staff (free of any contingency) together with a list of agreed rates against each grade; iii) a list of Costs underpinning those rates for each grade, being the agreed rate less the Supplier Profit Margin; and iv) Reimbursable Expenses, if allowed under the Order Form; c) Overheads; d) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables; e) the Supplier Profit achieved over the Framework Contract Period 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 Deliverables, including the amount of money attributed to each risk and/or contingency; and h) the actual Costs profile for each Service Period;
"Order"	means an order for the provision of the Deliverables placed by a Buyer with the Supplier under a Contract;
"Order Form"	a completed Order Form Template (or equivalent information issued by the Buyer) used to create a Call-Off Contract;
"Order Form Template"	the template in Framework Schedule 6 (Order Form Template and Call-Off Schedules);

Framework Ref: RM6116

Project Version: v1.0

Model Version: v3.10

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Other Contracting Authority"	any actual or potential Buyer under the Framework Contract;
"Overhead"	those amounts which are intended to recover a proportion of the Supplier's or the Key Subcontractor'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 Staff and accordingly included within limb (a) of the definition of "Costs";
"Parliament"	takes its natural meaning as interpreted by Law;
"Party"	in the context of the Framework Contract, CCS or the Supplier, and in the in the context of a Call-Off Contract the Buyer or the Supplier. "Parties" shall mean both of them where the context permits;
"Performance Indicators" or "PIs"	the performance measurements and targets in respect of the Supplier's performance of the Framework Contract set out in Framework Schedule 4 (Framework Management);
"Personal Data"	has the meaning given to it in the UK GDPR;
"Personal Data Breach"	has the meaning given to it in the UK GDPR;
"Personnel"	all directors, officers, employees, agents, consultants and suppliers of a Party and/or of any Subcontractor and/or Subprocessor engaged in the performance of its obligations under a Contract;
"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', 24 November 2016, 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 ;
Primary Services	the components described in paragraph 1.2.2 of Part A of Framework Schedule 1 (Specification);
"Processing"	has the meaning given to it in the UK GDPR;
"Processor"	has the meaning given to it in the UK GDPR;
"Progress Meeting"	a meeting between the Buyer Authorised Representative and the Supplier Authorised Representative;
"Progress Meeting Frequency"	the frequency at which the Supplier shall conduct a Progress Meeting in accordance with Clause 6.1 as specified in the Order Form;
"Progress Report"	a report provided by the Supplier indicating the steps taken to achieve Milestones or delivery dates;
"Progress Report Frequency"	the frequency at which the Supplier shall deliver Progress Reports in accordance with Clause 6.1 as specified in the Order Form;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Prohibited Acts"	<p>a) to directly or indirectly offer, promise or give any person working for or engaged by a Buyer or any other public body a financial or other advantage to:</p> <ul style="list-style-type: none"> 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; <p>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 each Contract; or</p> <p>c) committing any offence:</p> <ul style="list-style-type: none"> i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or ii) under legislation or common law concerning fraudulent acts; or iii) defrauding, attempting to defraud or conspiring to defraud a Buyer or other public body; or <p>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;</p>
"Protective Measures"	appropriate technical and organisational measures 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 Framework Schedule 9 (Cyber Essentials Scheme), if applicable, in the case of the Framework Contract or Call-Off Schedule 9 (Security), if applicable, in the case of a Call-Off Contract.
Public Services Network or PSN	the network of networks delivered through multiple service providers, as further detailed in the PSN operating model; and described at https://www.gov.uk/government/groups/public-services-network ;
Rating Agency	as defined in the Framework Award Form or the Order Form, as the context requires;
"Recall"	a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the right IPR rights) that might endanger health or hinder performance;
"Recipient Party"	the Party which receives or obtains directly or indirectly Confidential Information;

Framework Ref: RM6116

Project Version: v1.0

Model Version: v3.10

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Rectification Plan"	the Supplier's plan (or revised plan) to rectify it's breach using the template in Joint Schedule 10 (Rectification Plan) which shall include: a) full details of the Default that has occurred, including a root cause analysis; b) the actual or anticipated effect of the Default; and c) the steps which the Supplier proposes to take to rectify the Default (if applicable) and to prevent such Default from recurring, including timescales for such steps and for the rectification of the Default (where applicable);
"Rectification Plan Process"	the process set out in Clause 10.3.1 to 10.3.4 (Rectification Plan Process);
"Regulations"	the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires) as amended from time to time;
"Reimbursable Expenses"	the 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 Buyer's expenses policy current from time to time, but not including: a) travel expenses incurred as a result of Supplier Staff 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 Buyer otherwise agrees in advance in writing; and b) subsistence expenses incurred by Supplier Staff 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;
"Relevant Authority"	the Authority which is party to the Contract to which a right or obligation is owed, as the context requires;
"Relevant Authority's Confidential Information"	a) all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, property rights, trade secrets, Know-How and IPR of the Relevant Authority (including all Relevant Authority Existing IPR and New IPR); b) any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered confidential which comes (or has come) to the Relevant Authority's attention or into the Relevant Authority's possession in connection with a Contract; and information derived from any of the above;
"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 pursuant to section 9 of the Bribery Act 2010;

Framework Ref: RM6116

Project Version: v1.0

Model Version: v3.10

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Relevant Tax Authority"	HMRC, or, if applicable, the tax authority in the jurisdiction in which the Supplier is established;
"Reminder Notice"	a notice sent in accordance with Clause 10.5 given by the Supplier to the Buyer providing notification that payment has not been received on time;
"Replacement Deliverables"	any deliverables which are substantially similar to any of the Deliverables and which the Buyer receives in substitution for any of the Deliverables following the Call-Off Expiry Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Replacement Subcontractor"	a Subcontractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any Subcontractor of any such Subcontractor);
"Replacement Supplier"	any third party provider of Replacement Deliverables appointed by or at the direction of the Buyer from time to time or where the Buyer is providing Replacement Deliverables for its own account, shall also include the Buyer;
"Request For Information"	a request for information or an apparent request relating to a Contract for the provision of the Deliverables or an apparent request for such information under the FOIA or the EIRs;
"Required Insurances"	the insurances required by Joint Schedule 3 (Insurance Requirements) or any additional insurances specified in the Order Form;
RTI	Real Time Information
"Satisfaction Certificate"	the certificate (materially in the form of the document contained in of Part B of Call-Off Schedule 13 (Implementation Plan and Testing) or as agreed by the Parties where Call-Off Schedule 13 is not used in this Contract) granted by the Buyer when the Supplier has met all of the requirements of an Order, Achieved a Milestone or a Test;
"Security Management Plan"	the Supplier's security management plan prepared pursuant to Call-Off Schedule 9 (Security) (if applicable);
"Security Policy"	the Buyer's security policy, referred to in the Order Form, in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time and notified to the Supplier;
"Self Audit Certificate"	means the certificate in the form as set out in Framework Schedule 8 (Self Audit Certificate);
"Serious Fraud Office"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
"Service Levels"	any service levels applicable to the provision of the Deliverables under the Call Off Contract (which, where Call Off Schedule 14 (Service Levels) is used in this Contract, are specified in the Annex to Part A of such Schedule);
Service Offer	a Deliverable made available to Buyers by the Supplier via the Catalogue;

Framework Ref: RM6116

Project Version: v1.0

Model Version: v3.10

Joint Schedule 1 (Definitions)

Crown Copyright 2018

Service Offer Effective Date	the date when the Service Offer will be available to Buyers on the Catalogue;
Service Offer Expiry Date	the date the Service Offer will be/was removed from the Catalogue;
Service Offer Price Card	a list of prices, rates and other amounts for a specific Service Offer;
Service Offer Template	the template set out at Annex 1 to Part B of Framework Schedule 3 (Framework Prices);
"Service Period"	has the meaning given to it in the Order Form;
"Services"	services made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form;
"Service Transfer"	any transfer of the Deliverables (or any part of the Deliverables), for whatever reason, from the Supplier or any Subcontractor to a Replacement Supplier or a Replacement Subcontractor;
"Service Transfer Date"	the date of a Service Transfer;
"Sites"	any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: a) the Deliverables are (or are to be) provided; or b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables;
"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 enterprises;
Smart Cities (Smart share and connected spaces)	use of information, and communication technologies to increase operational efficiency, share information with the public and improve both the quality of government services and citizen welfare. Solutions in this area generally combine a number of technologies, including sensors for the collection of data, connectivity to cloud hosted data management platforms, and data visualisation applications.
"Special Terms"	any additional Clauses set out in the Framework Award Form or Order Form which shall form part of the respective Contract;
"Specific Change in Law"	a Change in Law that relates specifically to the business of the Buyer and which would not affect a Comparable Supply where the effect of that Specific Change in Law on the Deliverables is not reasonably foreseeable at the Start Date;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Specification"	the specification set out in Framework Schedule 1 (Specification), as may, in relation to a Call-Off Contract, be supplemented by the Order Form;
"Standards"	any: <ul style="list-style-type: none"> a) standards published by BSI British Standards, the National Standards Body of the United Kingdom, the International Organisation for Standardisation or other reputable or equivalent bodies (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with; b) standards detailed in the specification in Schedule 1 (Specification); c) standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time; d) relevant Government codes of practice and guidance applicable from time to time;
"Start Date"	in the case of the Framework Contract, the date specified on the Framework Award Form, and in the case of a Call-Off Contract, the date specified in the Order Form;
"Statement of Requirements"	a statement issued by the Buyer detailing its requirements in respect of Deliverables issued in accordance with the Call-Off Procedure;
"Storage Media"	the part of any device that is capable of storing and retrieving data;
"Sub-Contract"	any contract or agreement (or proposed contract or agreement), other than a Call-Off Contract or the Framework Contract, pursuant to which a third party: <ul style="list-style-type: none"> a) provides the Deliverables (or any part of them); b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);
"Subcontractor"	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
"Subprocessor"	any third Party appointed to process Personal Data on behalf of that Processor related to a Contract;
"Supplier"	the person, firm or company identified in the Framework Award Form;
Supplier Action Plan	a document, maintained by the Authority, capturing information about the relationship between the Parties including, but not limited to strategic objectives, actions, initiatives, communication channels, risks and supplier performance;

Framework Ref: RM6116

Project Version: v1.0

Model Version: v3.10

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Supplier Assets"	all assets and rights used by the Supplier to provide the Deliverables in accordance with the Call-Off Contract but excluding the Buyer Assets;
"Supplier Authorised Representative"	the representative appointed by the Supplier named in the Framework Award Form, or later defined in a Call-Off Contract;
"Supplier's Confidential Information"	<p>a) any information, however it is conveyed, that relates to the business, affairs, developments, IPR of the Supplier (including the Supplier Existing IPR) trade secrets, Know-How, and/or personnel of the Supplier;</p> <p>b) any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential and which comes (or has come) to the Supplier's attention or into the Supplier's possession in connection with a Contract;</p> <p>c) Information derived from any of (a) and (b) above;</p>
"Supplier's Contract Manager"	the person identified in the Order Form appointed by the Supplier to oversee the operation of the Call-Off Contract and any alternative person whom the Supplier intends to appoint to the role, provided that the Supplier informs the Buyer prior to the appointment;
"Supplier Equipment"	the Supplier's hardware, computer and telecoms devices, equipment, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from the Buyer) in the performance of its obligations under this Call-Off Contract;
"Supplier Marketing Contact"	shall be the person identified in the Framework Award Form;
"Supplier Non-Performance"	<p>where the Supplier has failed to:</p> <p>a) Achieve a Milestone by its Milestone Date;</p> <p>b) provide the Goods and/or Services in accordance with the Service Levels ; and/or</p> <p>c) comply with an obligation under a Contract;</p>
"Supplier Profit"	in relation to a period, the difference between the total Charges (in nominal cash flow terms but excluding any Deductions and total Costs (in nominal cash flow terms) in respect of a Call-Off Contract for the relevant period;
"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;
"Supplier Staff"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under a Contract;

Framework Ref: RM6116

Project Version: v1.0

Model Version: v3.10

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Supporting Documentation"	sufficient information in writing to enable the Buyer to reasonably assess whether the Charges, Reimbursable Expenses and other sums due from the Buyer under the Call-Off Contract detailed in the information are properly payable;
"Tax"	<p>a) all forms of taxation whether direct or indirect;</p> <p>b) national insurance contributions in the United Kingdom and similar contributions or obligations in any other jurisdiction;</p> <p>c) all statutory, governmental, state, federal, provincial, local government or municipal charges, duties, imports, contributions, levies or liabilities (other than in return for goods or services supplied or performed or to be performed) and withholdings; and</p> <p>d) any penalty, fine, surcharge, interest, charges or costs relating to any of the above,</p> <p>in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction;</p>
TEM Provider	a Supplier appointed by CCS to provide telecoms expense management;
"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 a Contract on a specified date and setting out the grounds for termination;
"Test Issue"	any variance or non-conformity of the Deliverables from their requirements as set out in a Call-Off Contract;
"Test Plan"	<p>a plan:</p> <p>a) for the Testing of the Deliverables; and</p> <p>b) setting out other agreed criteria related to the achievement of Milestones;</p>
"Tests "	any tests required to be carried out pursuant to a Call-Off Contract as set out in the Test Plan or elsewhere in a Call-Off Contract and "Tested" and "Testing" shall be construed accordingly;
"Third Party IPR"	Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables;
Time and Materials	a pricing mechanism whereby the Buyer agrees to pay the Supplier based upon the work performed by the Supplier's employees and Sub-Contractors, and for materials used in the project, no matter how much work is required to complete the project;
"Transferring Supplier Employees"	those employees of the Supplier and/or the Supplier's Subcontractors to whom the Employment Regulations will apply on the Service Transfer Date;

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Transparency Information"	the Transparency Reports and the content of a 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 Relevant Authority; and (ii) Commercially Sensitive Information;
"Transparency Reports"	the information relating to the Deliverables and performance of the Contracts which the Supplier is required to provide to the Buyer in accordance with the reporting requirements in Call-Off Schedule 1 (Transparency Reports);
TUPE	Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other regulations or UK legislation implementing the Acquired Rights Directive
United Kingdom	the country that consists of England, Scotland, Wales, and Northern Ireland
"Variation"	any change to a Contract;
"Variation Form"	the form set out in Joint Schedule 2 (Variation Form);
"Variation Procedure"	the procedure set out in Clause 24 (Changing the contract);
"VAT"	value added tax in accordance with the provisions of the Value Added Tax Act 1994;
"VCSE"	a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives;
"Worker"	any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables;
"Working Day"	any day other than a Saturday or Sunday or public holiday in England and Wales unless specified otherwise by the Parties in the Order Form;
"Work Day"	7.5 Work Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day; and
"Work Hours"	the hours spent by the Supplier Staff properly working on the provision of the Deliverables including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks.

Joint Schedule 2 (Variation Form)
Crown Copyright 2018

Joint Schedule 2 (Variation Form)

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the Contract)

Contract Details		
This variation is between:	[delete] as applicable: CCS / Buyer] ("CCS" "the Buyer") And [insert] name of Supplier] ("the Supplier")	
Contract name:	[insert] name of contract to be changed] ("the Contract")	
Contract reference number:	[insert] contract reference number]	
Details of Proposed Variation		
Variation initiated by:	[delete] as applicable: CCS/Buyer/Supplier]	
Variation number:	[insert] variation number]	
Date variation is raised:	[insert] date]	
Proposed variation		
Reason for the variation:	[insert] reason]	
An Impact Assessment shall be provided within:	[insert] number] days	
Impact of Variation		
Likely impact of the proposed variation:	[Supplier to insert] assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: <ul style="list-style-type: none"> [CCS/Buyer to insert] original Clauses or Paragraphs to be varied and the changed clause] 	
Financial variation:	Original Contract Value:	£ [insert] amount]
	Additional cost due to variation:	£ [insert] amount]
	New Contract value:	£ [insert] amount]

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by [delete] as applicable: CCS / Buyer]
2. Words and expressions in this Variation shall have the meanings given to them in the Contract.
3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Joint Schedule 2 (Variation Form)
Crown Copyright 2018

Signed by an authorised signatory for and on behalf of the **[delete]** as applicable: CCS / Buyer]

Signature

Date

Name (in Capitals)

Address

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature

Date

Name (in Capitals)

Address

Joint Schedule 2 (Variation Form)
Crown Copyright 2018

Joint Schedule 3 (Insurance Requirements)
Crown Copyright 2018

Joint Schedule 3 (Insurance Requirements)

1. The insurance you need to have

- 1.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under a Call-Off Contract (specified in the applicable Order Form) ("**Additional Insurances**") 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:
 - 1.1.1 the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and
 - 1.1.2 the Call-Off Contract Effective Date in respect of the Additional Insurances.
- 1.2 The Insurances shall be:
 - 1.2.1 maintained in accordance with Good Industry Practice;
 - 1.2.2 (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;
 - 1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and
 - 1.2.4 maintained for at least six (6) years after the End Date.
- 1.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

2. How to manage the insurance

- 2.1 Without limiting the other provisions of this Contract, the Supplier shall:
 - 2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables 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;
 - 2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and
 - 2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

Joint Schedule 3 (Insurance Requirements)

Crown Copyright 2018

3. What happens if you aren't insured

- 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 or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4. Evidence of insurance you must provide

- 4.1 The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

5. Making sure you are insured to the required amount

- 5.1 The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

6. Cancelled Insurance

- 6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.
- 6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

7. Insurance claims

- 7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

Joint Schedule 3 (Insurance Requirements)

Crown Copyright 2018

- 7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables 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 Relevant Authority) full details of the incident giving rise to the claim.
- 7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.
- 7.4 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 Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

Joint Schedule 3 (Insurance Requirements)

Crown Copyright 2018

ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following standard insurance cover from the Framework Start Date in accordance with this Schedule:
 - 1.1 professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000);
 - 1.2 public liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000); and
 - 1.3 employers' liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000).
 - 1.4 product liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000)

Joint Schedule 3 (Insurance Requirements)
Crown Copyright 2018

Joint Schedule 4 (Commercially Sensitive Information)

1. What is the Commercially Sensitive Information?

- 1.1 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.
- 1.2 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 and in the Order Form (which shall be deemed incorporated into the table below).
- 1.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 of the Core Terms (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

	From Date of Submission
	Vodafone's (VF) bid submission, proposal & commercial offering response to any ITT or potential opportunity, breakdown of pricing information to give input costs, capital & operating costs, overheads, revenue, margins & profits.
	Financial data relating to VF's business as a whole including the financial standing of VF & any information relating to financial distress reporting.
	The cover & amounts of VF's insurances.
	Technical details of VF's network including topology, network diagrams, detailed network coverage, route maps, VF's Points of Presence &/or street furniture/chambers etc.
	Design documents relating to the Services & any notes or minutes of technical design meetings held in relation to the aforementioned but excluding any documents set out in the Call Off Contract as being Deliverables.
	VF's Business Continuity Plan, Business Incident Plans, & Disaster Recovery Manuals & Procedures, Cyber Security Questionnaire, Security Plan & related Business Security Processes but excluding any Buyer-specific plans or procedures to be provided by VF under the Call Off Contract.
	From Call-Off Start Date
	How any payments due to VF on termination of the whole or any part of the Call Off Contract are calculated excluding the actual amounts.
	How service credits are calculated, but excluding any details regarding the applicable thresholds, any performance related information or requirements, information relating to the actual amounts of any service credits paid or credited. Duration for all the above: Expiry Date plus 6 years
	Details of the liability and indemnities provisions under the Call Off Contract;
	Staffing information including personal details.
	VF proposals in response to change requests.

Joint Schedule 4 (Commercially Sensitive Information)
Crown Copyright 2018

Joint Schedule 5 (Corporate Social Responsibility)
Crown Copyright 2018

Joint Schedule 5 (Corporate Social Responsibility)

Part A

1. Definitions

“Corporate Social Responsibility Reports”	written reports which the Supplier must complete and provide to the Buyer in accordance with Part B of this Schedule;
“Carbon Reduction Plan”	a plan which contains the details of emissions across a single year against a range of emissions sources and greenhouse gases, as per PPN 06/21;
“Modern Slavery Helpline”	means the mechanism for reporting suspicion, seeking help or advice and information on the subject of modern slavery available online at https://www.modernslaveryhelpline.org/report or by telephone on 08000 121 700;
“Prohibited Items”	means those items set out in Table A which the Supplier must not use in its performance of the Contract; and
“Waste Hierarchy”	<p>means prioritisation of waste management in the following order of preference:</p> <ul style="list-style-type: none"> prevention – by using less material in design and manufacture. Keeping products for longer; preparing for re-use – by checking, cleaning, repairing, refurbishing, whole items or spare parts; recycling – by turning waste into a new substance or produce, including composting if it meets quality protocols; other recovery – through anaerobic digestion, incineration with energy recovery, gasification and pyrolysis which produce energy (fuels, heat and power) and materials from waste; some backfilling; and disposal - Landfill and incineration without energy recovery.

Joint Schedule 5 (Corporate Social Responsibility)
Crown Copyright 2018

1. What we expect from our Suppliers

- 1.1 In February 2019, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government.
(https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779660/20190220-Supplier_Code_of_Conduct.pdf)
- 1.2 CCS expects its suppliers and subcontractors to meet the standards set out in that Code. In addition, CCS expects its suppliers and subcontractors to comply with the standards set out in this Schedule.
- 1.3 The Supplier acknowledges that the Buyer may have additional requirements in relation to corporate social responsibility. The Buyer expects that the Supplier and its Subcontractors will comply with such corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time.

2. Equality and Accessibility

- 2.1 In addition to legal obligations, the Supplier shall support CCS and the Buyer in fulfilling its Public Sector Equality duty under S149 of the Equality Act 2010 by ensuring that it fulfils its obligations under each Contract in a way that seeks to:
 - 2.1.1 eliminate discrimination, harassment or victimisation of any kind; and
 - 2.1.2 advance equality of opportunity and 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.

3. Modern Slavery, Child Labour and Inhumane Treatment

- 3.1 The Supplier:
 - 3.1.1 shall not use, nor allow its Subcontractors to use forced, bonded or involuntary prison labour;
 - 3.1.2 shall not require any Supplier Staff or Subcontractor Staff to lodge deposits or identify papers with the Employer and shall be free to leave their employer after reasonable notice;
 - 3.1.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world.
 - 3.1.4 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 offenses anywhere around the world.

Joint Schedule 5 (Corporate Social Responsibility)

Crown Copyright 2018

- 3.1.5 shall make reasonable enquires to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offenses anywhere around the world.
- 3.1.6 shall have and maintain throughout the term of each Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act and include in its contracts with its Subcontractors anti-slavery and human trafficking provisions;
- 3.1.7 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 a Contract;
- 3.1.8 shall prepare and deliver to CCS, 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 with its annual certification of compliance with Paragraph 3;
- 3.1.9 shall not use, nor allow its employees or Subcontractors 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 Subcontractors;
- 3.1.10 shall not use or allow child or slave labour to be used by its Subcontractors;
- 3.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to CCS, the Buyer and Modern Slavery Helpline.

4. Income Security

4.1 The Supplier shall:

- 4.1.1 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;
- 4.1.2 ensure that all Supplier Staff are provided with written and understandable Information about their employment conditions in respect of wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;
- 4.1.3 not make deductions from wages:
 - (a) as a disciplinary measure
 - (b) except where permitted by law; or
 - (c) without expressed permission of the worker concerned;
- 4.1.4 record all disciplinary measures taken against Supplier Staff; and
- 4.1.5 ensure that Supplier Staff are engaged under a recognised employment relationship established through national law and practice.

Joint Schedule 5 (Corporate Social Responsibility)

Crown Copyright 2018

5. Working Hours

5.1 The Supplier shall:

- 5.1.1 ensure that the working hours of Supplier Staff comply with national laws, and any collective agreements;
- 5.1.2 that the working hours of Supplier Staff, excluding overtime, shall be defined by contract, and shall not exceed 48 hours per week unless the individual has agreed in writing;
- 5.1.3 ensure that use of overtime used responsibly, taking into account:
 - (a) the extent;
 - (b) frequency; and
 - (c) hours worked;

by individuals and by the Supplier Staff as a whole;

5.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.

5.3 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:

- 5.3.1 this is allowed by national law;
- 5.3.2 this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce
- 5.3.3 appropriate safeguards are taken to protect the workers' health and safety; and
- 5.3.4 the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.

5.4 All Supplier Staff 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.

6. Environmental Requirements

- 6.1. The Supplier shall comply in all material respects with all applicable environmental laws, permits and regulations in force in relation to the Contract.

Joint Schedule 5 (Corporate Social Responsibility)

Crown Copyright 2018

- 6.2. The Supplier warrants that it has complied with the principles of ISO 14001 standards throughout the Term.
- 6.3. The Supplier shall meet the Government Buying Standards applicable to the Deliverables which can be found online at:
<https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs>.

Part B – Sustainability and Reporting

1. Sustainability Requirements

- 1.1 The Supplier shall complete the Corporate Social Responsibility Report at Paragraph 3 of this Part B in relation to its provision of the Deliverables under this Contract and provide the Corporate Social Responsibility Report to the Buyer on the date and frequency outlined in Table A of this Part B.
- 1.2 The Supplier shall use reasonable endeavours to avoid the use of paper and card in carrying out its obligations under this Contract. Where unavoidable under reasonable endeavours, the Supplier shall ensure that any paper or card deployed in the performance of the Services consists of one hundred percent (100%) recycled content and used on both sides where feasible to do so.
- 1.3 The Supplier shall complete and provide CCS with a Carbon Reduction Plan.
- 1.4 The Supplier shall progress towards carbon net zero during the lifetime of the framework.

2. Social Value Requirements

- 2.1 The Supplier shall complete the Corporate Social Responsibility Report at Paragraph 3 of this Part B in relation its performance on meeting any Social Value obligations agreed to for the provision of the Deliverables under this Contract and provide the Corporate Social Responsibility Report to the Buyer on the date and frequency outlined in Table A of this Part B.
- 2.2 The Supplier shall use its best endeavours, as an organisation, to deliver environmental sustainability and protection in the provision of the Deliverables by establishing and delivering against credible targets for delivering energy efficiency throughout the lifetime of the framework.
- 2.3 The Supplier shall use its best endeavours, as an organisation, to address inequality in employment, skills and pay by supporting disadvantaged, underrepresented and minority groups into employment throughout the lifetime of the framework.
- 2.4 The Supplier shall use its best endeavours, as an organisation, to promote new opportunities and engage with new and small organisations (e.g. SMEs and VCSEs), to help them grow, supporting their development throughout the lifetime of the framework.

Joint Schedule 5 (Corporate Social Responsibility)

Crown Copyright 2018

3. Reporting Requirements

- 3.1 The Supplier shall complete the Corporate Social Responsibility Report in relation to its provision of the Deliverables under this Contract and provide the Corporate Social Responsibility Report to the Buyer on the date and frequency outlined in Table A of this Part B.
- 3.2 The Supplier shall provide the baseline data contained within table B(1) – Baseline data to facilitate subsequent measurement throughout the lifetime of the framework. The information required to populate table B(1) and annually thereafter will be provided to CCS within 10 calendar days of the submission of a request by CCS.
- 3.3 The Supplier shall complete the Framework Performance Indicator Submission Form at the frequency outlined in Table B of this Part B and return to CCS. The Supplier shall include in the Framework Performance Indicator Submission Form the content specified within Table B.
- 3.4 The Supplier shall attend Supplier Relationship Meetings with CCS at such times and frequencies as CCS determines from time to time to discuss the information contained in the Framework Performance Indicator Submission Forms. The information will be used to measure progress of social value activity.
- 3.5 In the event CCS develops an alternative social value measurement tool during the lifetime of the framework, the Performance Indicator measures described at Table B will be superseded by that tool.

Joint Schedule 5 (Corporate Social Responsibility)

Crown Copyright 2018

Table A

Report Name	Content of Report	Frequency of Report
Sustainability	<ul style="list-style-type: none"> a. the key sustainability impacts identified; b. sustainability improvements made; c. actions underway or planned to reduce sustainability impacts; d. contributions made to the Buyer's sustainability policies and objectives; e. sustainability policies, standards, targets and practices that have been adopted to reduce the environmental impact of the Supplier's operations and evidence of these being actively pursued, indicating arrangements for engagement and achievements. This can also include where positive sustainability impacts have been delivered; and f. risks to the Service and Subcontractors of climate change and severe weather events such as flooding and extreme temperatures including mitigation, adaptation and continuity plans employed by the Supplier in response to those risks. 	On the anniversary of the Effective Date
Greenhouse Gas Emissions	Indicate greenhouse gas emissions making use of the use of the most recent conversion guidance set out in 'Greenhouse gas reporting – Conversion factors' available online at https://www.gov.uk/guidance/measuring-and-reporting-environmental-impacts-guidance-for-businesses	On the anniversary of the Effective Date

Joint Schedule 5 (Corporate Social Responsibility)
Crown Copyright 2018

Water Use	Volume in metres cubed.	On the anniversary of the Effective Date
Energy Use	<p>Separate energy consumption figures for:</p> <ol style="list-style-type: none"> assets deployed on the Supplier's site; assets deployed on the Authority's site; assets deployed off-site; and energy consumed by IT assets and by any cooling devices deployed. <p>Power Usage Effectiveness (PUE) rating for each data centre/server room in accordance with ISO/IEC 31034-2/EN 50600-4-2.</p>	On the anniversary of the Effective Date
Social Value	Details of any relevant Social Value requirements	On the anniversary of the Effective Date

Table B – Submission to CCS

Report Name	Content of Report	Frequency of Report
Framework Performance Indicator Submission Form – Modern Slavery section	<p>MSAT completion and progress recorded against the following 6 areas:</p> <ul style="list-style-type: none"> ● Governance ● Policies and Procedures ● Risk Assessment and Management ● Due Diligence 	Annually

Joint Schedule 5 (Corporate Social Responsibility)

Crown Copyright 2018

	<ul style="list-style-type: none"> • Training • KPI 	
Framework Performance Indicator Submission Form – Carbon Net Zero	<p>The Supplier to demonstrate progression towards carbon net zero by reporting on the below areas</p> <ul style="list-style-type: none"> • Number of carbon reduction activities that your organisation has taken to progress your carbon reduction plan • Number of RM6116 carbon reduction activities that benefit the Buyer • List the top 3 carbon reduction activities completed for non RM6116 contracts 	Annually
Framework Performance Indicator Submission Form – Apprenticeships	<p>Supplier shall submit data demonstrating how they are progressing apprenticeships within their organisation</p> <ul style="list-style-type: none"> • Number of apprenticeships started • Cumulative number of apprenticeships ongoing • Number of apprenticeships concluded • Number of apprenticeships retained 	Annually
Framework Performance Indicator Submission Form – Diversity & Inclusion	<p>To demonstrate that suppliers are redressing workforce imbalance within their organisation</p> <ul style="list-style-type: none"> • Representation of women • Representation of ethnic minorities • Representation of staff who identify as having a disability • Representation of prison leavers • Representation of LBTQIA+ 	Annually

Joint Schedule 5 (Corporate Social Responsibility)

Crown Copyright 2018

Framework Performance Indicator Submission Form – SMEs/VCSEs	<p>To demonstrate that Suppliers are engaging with and developing SMEs/VCSES</p> <ul style="list-style-type: none"> • Number of SMEs/VCSES within your supply chain for RM6116 • Number of SME/VCSEs within your supply chain delivering services on RM6116 contracts • How many sub-contract opportunities have there been within the reporting period • Of the sub-contract opportunities, how many were awarded to a SMEs 	Annually
--	--	----------

Table B(1) – Baseline data

Report Name	Content of Report	Frequency of Report
Apprenticeships baseline data	<p>The Supplier shall submit data demonstrating:</p> <ul style="list-style-type: none"> • % of apprentices in their current workforce • % conversion rate of apprentices retained when an apprenticeship concludes 	To be provided to CCS within 10 calendar days of the submission of a request and annually thereafter
Diversity of Workforce baseline data	<p>The Supplier shall submit baseline figures of their current UK workforce:</p> <ul style="list-style-type: none"> • Representation of women • Representation of ethnic minorities • Representation of staff who identify as having a disability 	To be provided to CCS within 10 calendar days of the submission of a request and annually thereafter

Framework Ref: RM6116

Project Version: v1.0

Model Version: v3.2

Joint Schedule 5 (Corporate Social Responsibility)

Crown Copyright 2018

	<ul style="list-style-type: none"> • Representation of prison leavers • Representation of LBTQIA+ 	
SMEs/VCSEs baseline data	The Supplier shall produce and submit a SME / VCSE engagement strategy detailing how they intend to retain and develop SMEs/VCSEs within their supply chain.	To be provided to CCS within 10 calendar days of the submission of a request and annually thereafter

Joint Schedule 10 (Rectification Plan)
Crown Copyright 2018

Joint Schedule 10 (Rectification Plan)

Request for [Revised] Rectification Plan		
Details of the Default:	[Guidance: Explain the Default, with clear schedule and clause references as appropriate]	
Deadline for receiving the [Revised] Rectification Plan:	[add date (minimum 10 days from request)]	
Signed by [CCS/Buyer] :		Date:
Supplier [Revised] Rectification Plan		
Cause of the Default	[add cause]	
Anticipated impact assessment:	[add impact]	
Actual effect of Default:	[add effect]	
Steps to be taken to rectification:	Steps	Timescale
	1.	[date]
	2.	[date]
	3.	[date]
	4.	[date]
	[...]	[date]
Timescale for complete Rectification of Default	[X] Working Days	
Steps taken to prevent recurrence of Default	Steps	Timescale
	1.	[date]
	2.	[date]
	3.	[date]
	4.	[date]
	[...]	[date]

Joint Schedule 10 (Rectification Plan)

Crown Copyright 2018

Signed by the Supplier:		Date:	
Review of Rectification Plan [CCS/Buyer]			
Outcome of review	[Plan Accepted] [Plan Rejected] [Revised Plan Requested]		
Reasons for Rejection (if applicable)	[add reasons]		
Signed by [CCS/Buyer]		Date:	

Joint Schedule 11 (Processing Data)
Crown Copyright 2018

Joint Schedule 11 (Processing Data)

Definitions

1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

“Processor Personnel” all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;

Status of the Controller

2. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

- (a) “Controller” in respect of the other Party who is “Processor”;
- (b) “Processor” in respect of the other Party who is “Controller”;
- (c) “Joint Controller” with the other Party;
- (d) “Independent Controller” of the Personal Data where the other Party is also “Controller”,

in respect of certain Personal Data under a Contract and shall specify in Annex 1 of this Joint Schedule 11 (*Processing Personal Data*) which scenario they think shall apply in each situation.

Where one Party is Controller and the other Party its Processor

3. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 of this Joint Schedule 11 (*Processing Personal Data*) by the Controller.
4. The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.
5. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:
 - (a) a systematic description of the envisaged Processing and the purpose of the Processing;
 - (b) an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
 - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and

Joint Schedule 11 (Processing Data)

Crown Copyright 2018

- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
6. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
- (a) Process that Personal Data only in accordance with Annex 1 of this Joint Schedule 11 (*Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
 - (b) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Personal Data Breach;
 - (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 the Contract (and in particular Annex 1 of this Joint Schedule 11 (*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 Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;
 - (B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
 - (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 the Contract; and
 - (D) have undergone adequate training in the use, care, protection and handling of Personal Data;
 - (d) not transfer Personal Data outside of the UK or European Economic Area unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
 - (i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;

Framework Ref: RM6116

Project Version: v1.0

Model Version: v4.5

Joint Schedule 11 (Processing Data)

Crown Copyright 2018

- (ii) the Data Subject has enforceable rights and effective legal remedies;
 - (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
 - (iv) 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.
7. Subject to paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:
- (a) receives a Data Subject Access Request (or purported Data Subject Access 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 the 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 Personal Data Breach.
8. The Processor's obligation to notify under paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
9. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 7 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately 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 Access Request within the relevant timescales set out in the Data Protection Legislation;

Joint Schedule 11 (Processing Data)

Crown Copyright 2018

- (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 Personal Data Breach; and/or
 - (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.
10. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. 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.
 11. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
 12. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
 13. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
 - (a) notify the Controller in writing of the intended Subprocessor and Processing;
 - (b) obtain the written consent of the Controller;
 - (c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and
 - (d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
 14. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
 15. The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).
 16. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Framework Ref: RM6116

Project Version: v1.0

Model Version: v4.5

Joint Schedule 11 (Processing Data)

Crown Copyright 2018

Where the Parties are Joint Controllers of Personal Data

17. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11.

Independent Controllers of Personal Data

18. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
19. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
20. Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
21. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
22. The Parties shall only provide Personal Data to each other:
 - (a) to the extent necessary to perform their respective obligations under the Contract;
 - (b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and
 - (c) where it has recorded it in Annex 1 of this Joint Schedule 11 (*Processing Personal Data*).
23. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.
24. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK

Framework Ref: RM6116

Project Version: v1.0

Model Version: v4.5

Joint Schedule 11 (Processing Data)

Crown Copyright 2018

GDPR and shall make the record available to the other Party upon reasonable request.

25. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract (**“Request Recipient”**):
 - (a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
 - (b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
 - (i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
 - (ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
26. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:
 - (a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
 - (b) implement any measures necessary to restore the security of any compromised Personal Data;
 - (c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
 - (d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.
27. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 of this Joint Schedule 11 (*Processing Personal Data*).
28. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 of this Joint Schedule 11 (*Processing Personal Data*).

Joint Schedule 11 (Processing Data)

Crown Copyright 2018

29. Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 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 paragraphs 18 to 28 of this Joint Schedule 11.

Joint Schedule 11 (Processing Data)

Crown Copyright 2018

Annex 1 - Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

- 1.1 The contact details of the Relevant Authority's Data Protection Officer are: as listed on the Relevant Authority's website
- 1.2 The contact details of the Supplier's Data Protection Officer are: data.protection@vodafone.com
- 1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	<p>The Relevant Authority is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that the Supplier is not acting in the capacity of the Relevant Authority's Processor for Personal Data Processed for the Services in the Service Offer, and so paragraph 3 to paragraph 16 of this Joint Schedule 11 do not apply to the Processing of Personal Data for the Services in the Service Offer.</p> <p>The Supplier is Controller and the Relevant Authority is Processor</p> <p>The Parties acknowledge that the Relevant Authority is not acting in the capacity of the Supplier's Processor for Personal Data Processed for the Services in the Service Offer, and so paragraph 3 to paragraph 16 of this Joint Schedule 11 do not apply to the Processing of Personal Data for the Services in the Service Offer.</p> <p>The Parties are Joint Controllers</p> <p>The Parties acknowledge that they do not act in the capacity of Joint Controllers to each other for Personal Data Processed for the Services in the Service Offer, and so paragraph 17 and Annex 2 of this Joint Schedule 11 does not apply to the Processing of Personal Data for the Services in the Service Offer.</p> <p>The Parties are Independent Controllers of Personal Data</p> <p>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of the following for Personal Data Processed for the Services in the Service Offer:</p> <ul style="list-style-type: none"> ● "Operational Data", which may include:

Joint Schedule 11 (Processing Data)
Crown Copyright 2018

	<ul style="list-style-type: none"> ○ Business contact details of Supplier Personnel, and any other Personal Data incidentally processed operationally for the performance of the Call off Contract, for which the Supplier is the Independent Controller; ○ Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract), any other Personal Data incidentally processed operationally for the performance of the Call off Contract for which the Relevant Authority is the Independent Controller; and ○ any Personal Data that is processed incidentally as part of a standardised service is such that the Relevant Authority cannot dictate the way in which Personal Data is processed by the Supplier, for which the Supplier is the Independent Controller. <ul style="list-style-type: none"> ● As outlined in Paragraph 29, where the Supplier has professional or regulatory obligations in respect of Personal Data Processed for the provision of the Services in the Service Offer, including Traffic Data, for which the Supplier shall be an Independent Controller. Traffic Data shall mean any data processed for the purpose of the conveyance of a communication on electronic communications network and for billing, which may include Personal Data.
Duration of the Processing	<p>As they are acting as an Independent Controller, the Supplier's processing of Personal Data shall be in accordance with its privacy policy.</p> <p>As they are acting as an Independent Controller, Relevant Authority's processing of Operational Data shall be in accordance with Relevant Authority's privacy policy.</p>
Nature and purposes of the Processing	<p><u>Nature of the processing</u>: collection, recording, organisation, structuring, storage (including hosting), analysis, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) and any other purpose stated within the Service Offer.</p> <p><u>Purpose</u>: the provision and operation of the Service Offer.</p>
Type of Personal Data	<p><u>Operational Data may include the following</u>: Business contact information such as name, email address, work address, telephone and fax numbers, gender, title, security clearances and related security measures, e-signature, user account and identity verification information, complaints and escalations, customer care</p>

Joint Schedule 11 (Processing Data)

Crown Copyright 2018

	<p>contact information, requests for access to personal data, correspondence relating to customer care, cookies, mobile device identifiers, serial number/SIM card number, pseudonymous profiles, marketing preferences, emails from and to Relevant Authority's users relating to the Service, device-based or device-related data for corporate devices and any other category of Personal Data as stated within the Service Offer.</p> <p><u>Traffic Data may include the following:</u> Network/Services usage information, such as IP address, call information (duration, start/end time), network events/activity logs/browsing logs, TAP files, volume (i.e. amount of mins/SMS), location data and system access or audit logs and any other purpose stated within the Service Offer.</p>
Categories of Data Subject	In respect of Operational Data and Traffic Data, the other Party's employees or representatives.
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	<p>As they are acting as an Independent Controller, the Relevant Authority's retention and destruction of the Personal Data shall be in accordance with its privacy policy.</p> <p>As they are acting as an Independent Controller, the Supplier's retention and destruction of the Personal Data shall be in accordance with its privacy policy.</p>

Joint Schedule 11 (Processing Data)

Crown Copyright 2018

Annex 2 - Joint Controller Agreement

Intentionally Blank – The Parties acknowledge that they do not act in the capacity of Joint Controllers to each other for Personal Data Processed for the Services in the Service Offer, and so paragraph 17 and Annex 2 of this Joint Schedule 11 does not apply to the Processing of Personal Data for the Services in the Service Offer.

Call-Off Schedule 1 (Transparency Reports)

Call-Off Ref:

Crown Copyright 2018

Call-Off Schedule 1 (Transparency Reports)

- 1.1 The Supplier recognises that the Buyer is subject to PPN 01/17 (Updates to transparency principles v1.1 (<https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles>)). The Supplier shall comply with the provisions of this Schedule in order to assist the Buyer with its compliance with its obligations under that PPN.
- 1.2 Without prejudice to the Supplier's reporting requirements set out in the Framework Contract, within three (3) Months of the Start Date the Supplier shall submit to the Buyer for Approval (such Approval not to be unreasonably withheld or delayed) draft Transparency Reports consistent with the content requirements and format set out in the Annex of this Schedule.
- 1.3 If the Buyer rejects any proposed Transparency Report submitted by the Supplier, the Supplier shall submit a revised version of the relevant report for further Approval 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 Buyer. If the Parties fail to agree on a draft Transparency Report the Buyer shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.
- 1.4 The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Buyer at the frequency referred to in the Annex of this Schedule.

Call-Off Schedule 1 (Transparency Reports)

Call-Off Ref:

Crown Copyright 2018

Annex A: List of Transparency Reports

Title	Content	Format	Frequency
Call-Off Contract Charges Information Report	As per Supplier's standard report	Assessable for Lots via https://myenterprise.vodafone.co.uk:8443/oneportal/	Once within three (3) months of the Call Off Start Date only
Key Subcontractors	As set out in the Service Offer	The list set out in the Service Offer	Call-Off Start Date only

Call-Off Schedule 1 (Transparency Reports)
Call-Off Ref:
Crown Copyright 2018

Call-Off Schedule 2 (Staff Transfer)
Call-Off Ref:
Crown Copyright 2018

Call-Off Schedule 2 (Staff Transfer)

1. Definitions

1.1 In this Schedule, the following words have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

- “Acquired Rights Directive”**

1 the European Council Directive 77/187/EEC on the approximation of laws of European member states relating to the safeguarding of employees’ rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses, as amended or re-enacted from time to time;
- “Employee Liability”**

2
3 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 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;

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2018

- 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;

"Former Supplier"

a supplier supplying services to the Buyer before the Relevant Transfer Date that are the same as or substantially similar to the Services (or any part of the Services) and shall include any Subcontractor of such supplier (or any Subcontractor of any such Subcontractor);

"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:

- (i) any amendments to that document immediately prior to the Relevant Transfer Date; and
- (ii) any similar pension protection in accordance with the Annexes D1-D3 inclusive to Part D of this Schedule as notified to the Supplier by the Buyer;

"Old Fair Deal"

HM Treasury Guidance *"Staff Transfers from Central Government: A Fair Deal for Staff Pensions"* issued in June 1999 including the supplementary guidance *"Fair Deal for Staff pensions: Procurement of Bulk Transfer Agreements and Related Issues"* issued in June 2004;

"Partial Termination"

the partial termination of the relevant Contract to the extent that it relates to the provision of any part of the Services as further provided for in Clause 10.4 (When CCS or the Buyer can end this contract) or 10.6 (When the Supplier can end the contract);

"Relevant Transfer"

a transfer of employment to which the Employment Regulations applies;

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2018

"Relevant Transfer Date"

in relation to a Relevant Transfer, the date upon which the Relevant Transfer takes place. For the purposes of Part D: Pensions and its Annexes, where the Supplier or a Subcontractor was the Former Supplier and there is no Relevant Transfer of the Fair Deal Employees because they remain continuously employed by the Supplier (or Subcontractor), references to the Relevant Transfer Date shall become references to the Start Date;

"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, such information as the Buyer may reasonably request (subject to all applicable provisions of the Data Protection Legislation), but including in an anonymised format:

- (a) their ages, dates of commencement of employment or engagement, gender and place of work;
- (b) details of whether they are employed, self-employed contractors or consultants, agency workers or otherwise;
- (c) the identity of the employer or relevant contracting Party;
- (d) their relevant contractual notice periods and any other terms relating to termination of employment, including redundancy procedures, and redundancy payments;
- (e) their wages, salaries, bonuses and profit sharing arrangements as applicable;
- (f) details of other employment-related benefits, including (without limitation) medical insurance, life assurance, pension or other retirement benefit schemes, share option schemes and company car schedules applicable to them;
- (g) any outstanding or potential contractual, statutory or other liabilities in respect of such individuals (including in respect of personal injury claims);

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2018

- (h) details of any such individuals on long term sickness absence, parental leave, maternity leave or other authorised long term absence;
- (i) copies of all relevant documents and materials relating to such information, including copies of relevant contracts of employment (or relevant standard contracts if applied generally in respect of such employees); and
- (j) any other "employee liability information" as such term is defined in regulation 11 of the Employment Regulations;

"Supplier's Final Supplier Personnel List"	a list provided by the Supplier of all Supplier Staff whose 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 Staff 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;
"Term"	the period commencing on the Start Date and ending on the expiry of the Initial Period or any Extension Period or on earlier termination of the relevant Contract;
"Transferring Buyer Employees"	those employees of the Buyer to whom the Employment Regulations will apply on the Relevant Transfer Date;
"Transferring Former Supplier Employees"	in relation to a Former Supplier, those employees of the Former Supplier to whom the Employment Regulations will apply on the Relevant Transfer Date.

2. INTERPRETATION

- 2.1 Where a provision in this Schedule imposes any obligation on the Supplier including (without limit) to comply with a requirement or provide an indemnity, undertaking or warranty, the Supplier shall procure that each of its Subcontractors shall comply with such obligation and provide such indemnity, undertaking or warranty to CCS, the Buyer, Former Supplier, Replacement Supplier or Replacement Subcontractor, as the case may be and where the Subcontractor fails to satisfy any claims under such indemnities the Supplier

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2018

will be liable for satisfying any such claim as if it had provided the indemnity itself.

- 2.2 The provisions of Paragraphs 2.1 and 2.6 of Part A, Paragraph 3.1 of Part B, Paragraphs 1.5, 1.7 and 1.9 of Part C, Part D and Paragraphs 1.4, 2.3 and 2.8 of Part E of this Schedule (together “Third Party Provisions”) confer benefits on third parties (each such person a “Third Party Beneficiary”) and are intended to be enforceable by Third Party Beneficiaries by virtue of the CRTPA.
- 2.3 Subject to Paragraph 2.2 above, a person who is not a Party to this Call-Off Contract has no right under the CRTPA to enforce any term of this Call-Off Contract but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.
- 2.4 No Third Party Beneficiary may enforce, or take any step to enforce, any Third Party Provision without the prior written consent of the Buyer, which may, if given, be given on and subject to such terms as the Buyer may determine.
- 2.5 Any amendments or modifications to this Call-Off Contract may be made, and any rights created under Paragraph 2.2 above may be altered or extinguished, by the Parties without the consent of any Third Party Beneficiary.

3. Which parts of this Schedule apply

Only the following parts of this Schedule shall apply to this Call Off Contract:

- Part C (No Staff Transfer on the Start Date)
- Part E (Staff Transfer on Exit)

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2018

PART C: NO STAFF TRANSFER ON THE START DATE

1. What happens if there is a staff transfer

- 1.1 The Buyer and the Supplier agree that the commencement of the provision of the Services or of any part of the Services will not be a Relevant Transfer in relation to any employees of the Buyer and/or any Former Supplier.
- 1.2 If any employee of the Buyer and/or a Former Supplier claims, or it is determined in relation to any employee of the Buyer and/or a Former Supplier, that his/her contract of employment has been transferred from the Buyer and/or the Former Supplier to the Supplier and/or any Subcontractor pursuant to the Employment Regulations or the Acquired Rights Directive then:
 - 1.2.1 the Supplier shall, and shall procure that the relevant Subcontractor shall, within 5 Working Days of becoming aware of that fact, notify the Buyer in writing and, where required by the Buyer, notify the Former Supplier in writing; and
 - 1.2.2 the Buyer and/or 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 from the Supplier or the Subcontractor (as appropriate) or take such other reasonable steps as the Buyer or Former Supplier (as the case may be) it 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 1.2.2 is accepted (or if the situation has otherwise been resolved by the Buyer and/or the Former Supplier),, the Supplier shall, or shall procure that the Subcontractor shall, immediately release the person from his/her employment or alleged employment.
- 1.4 If by the end of the 15 Working Day period referred to in Paragraph 1.2.2:
 - 1.4.1 no such offer of employment has been made;
 - 1.4.2 such offer has been made but not accepted; or
 - 1.4.3 the situation has not otherwise been resolved;

the Supplier may within 5 Working Days give notice to terminate the employment or alleged employment of such person.
- 1.5 Subject to the Supplier and/or the relevant Subcontractor 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 1.8 the Buyer shall:
 - 1.5.1 indemnify the Supplier and/or the relevant Subcontractor against all Employee Liabilities arising out of the termination of the employment of any of the Buyer's employees referred to in Paragraph 1.2 made pursuant to the provisions of Paragraph 1.4

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2018

- provided that the Supplier takes, or shall procure that the Subcontractor takes, all reasonable steps to minimise any such Employee Liabilities; and
- 1.5.2 procure that the Former Supplier indemnifies the Supplier and/or any Subcontractor against all Employee Liabilities arising out of termination of the employment of the employees of the Former Supplier 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 Subcontractor takes, all reasonable steps to minimise any such Employee Liabilities.
- 1.6 If any such person as is described in Paragraph 1.2 is neither re employed by the Buyer and/or the Former Supplier as appropriate nor dismissed by the Supplier and/or any Subcontractor within the 15 Working Day period referred to in Paragraph 1.4 such person shall be treated as having transferred to the Supplier and/or the Subcontractor (as appropriate) and the Supplier shall, or shall procure that the Subcontractor shall, comply with such obligations as may be imposed upon it under Law.
- 1.7 Where any person remains employed by the Supplier and/or any Subcontractor pursuant to Paragraph 1.6, all Employee Liabilities in relation to such employee shall remain with the Supplier and/or the Subcontractor and the Supplier shall indemnify the Buyer and any Former Supplier, and shall procure that the Subcontractor shall indemnify the Buyer and any Former Supplier, against any Employee Liabilities that either of them may incur in respect of any such employees of the Supplier and/or employees of the Subcontractor.
- 1.8 The indemnities in Paragraph 1.5:
- 1.8.1 shall not apply to:
- (a) any claim for:
- (i) discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief; or
- (ii) 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 and/or Subcontractor; or
- (b) any claim that the termination of employment was unfair because the Supplier and/or any Subcontractor neglected to follow a fair dismissal procedure; and
- 1.8.2 shall apply only where the notification referred to in Paragraph 1.2.1 is made by the Supplier and/or any

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2018

Subcontractor to the Buyer and, if applicable, Former Supplier within 6 months of the Start Date.

- 1.9 If the Supplier and/or the Subcontractor does not comply with Paragraph 1.2, all Employee Liabilities in relation to such employees shall remain with the Supplier and/or the Subcontractor and the Supplier shall (i) comply with the provisions of Part D: Pensions of this Schedule, and (ii) indemnify the Buyer and any Former Supplier against any Employee Liabilities that either of them may incur in respect of any such employees of the Supplier and/or employees of the Subcontractor.

2. Limits on the Former Supplier's obligations

Where in this Part C the Buyer 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 Buyer's contract with the Former Supplier contains a contractual right in that regard which the Buyer may enforce, or otherwise so that it requires only that the Buyer must use reasonable endeavours to procure that the Former Supplier does or does not act accordingly.

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2018

Part E: Staff Transfer on Exit

1. Obligations before a Staff Transfer

1.1 The Supplier agrees that within 20 Working Days of the earliest of:

- 1.1.1 receipt of a notification from the Buyer of a Service Transfer or intended Service Transfer;
- 1.1.2 receipt of the giving of notice of early termination or any Partial Termination of the relevant Contract;
- 1.1.3 the date which is 12 Months before the end of the Term; and
- 1.1.4 receipt of a written request of the Buyer at any time (provided that the Buyer 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 Data Protection Legislation, the Supplier's Provisional Supplier Personnel List, together with the Staffing Information in relation to the Supplier's Provisional Supplier Personnel List and it shall provide an updated Supplier's Provisional Supplier Personnel List at such intervals as are reasonably requested by the Buyer.

1.2 At least 20 Working Days prior to the Service Transfer Date, the Supplier shall provide to the Buyer or at the direction of the Buyer to any Replacement Supplier and/or any Replacement Subcontractor (i) the Supplier's Final Supplier Personnel List, which shall identify the basis upon which they are Transferring Supplier Employees and (ii) 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 Buyer 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 and/or Replacement Subcontractor.

1.4 The Supplier warrants, for the benefit of The Buyer, any Replacement Supplier, and any Replacement Subcontractor that all information provided pursuant to Paragraphs 1.1 and 1.2 shall be 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 1.1.1, 1.1.2 and 1.1.3, the Supplier agrees that it shall not, and agrees to procure that each Subcontractor 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 approval of the Buyer (not to be unreasonably withheld or delayed):

:

- 1.5.1 replace or re-deploy any Supplier Staff listed on the Supplier Provisional Supplier Personnel List other than where any

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2018

- replacement is of equivalent grade, skills, experience and expertise and is employed on the same terms and conditions of employment as the person he/she replaces
- 1.5.2 make, promise, propose, permit or implement any material changes to the terms and conditions of employment of the Supplier Staff (including pensions and any payments connected with the termination of employment);
 - 1.5.3 increase the proportion of working time spent on the Services (or the relevant part of the Services) by any of the Supplier Staff save for fulfilling assignments and projects previously scheduled and agreed;
 - 1.5.4 introduce any new contractual or customary practice concerning the making of any lump sum payment on the termination of employment of any employees listed on the Supplier's Provisional Supplier Personnel List;
 - 1.5.5 increase or reduce the total number of employees so engaged, or deploy any other person to perform the Services (or the relevant part of the Services);
 - 1.5.6 terminate or give notice to terminate the employment or contracts of any persons on the Supplier's Provisional Supplier Personnel List save by due disciplinary process;
- and shall promptly notify, and procure that each Subcontractor shall promptly notify, the Buyer or, at the direction of the Buyer, any Replacement Supplier and any Replacement Subcontractor of any notice to terminate employment given by the Supplier or relevant Subcontractor or received from any persons listed on the Supplier's Provisional Supplier Personnel List regardless of when such notice takes effect.
- 1.6 On or around each anniversary of the Start Date and up to four times during the last 12 Months of the Term, the Buyer may make written requests to the Supplier for information relating to the manner in which the Services are organised. Within 20 Working Days of receipt of a written request the Supplier shall provide, and shall procure that each Subcontractor shall provide, to the Buyer such information as the Buyer may reasonably require relating to the manner in which the Services are organised, which shall include:
 - 1.6.1 the numbers of employees engaged in providing the Services;
 - 1.6.2 the percentage of time spent by each employee engaged in providing the Services;
 - 1.6.3 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 any of the Annexes to Part D (Pensions) (as appropriate); and
 - 1.6.4 a description of the nature of the work undertaken by each employee by location.

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2018

- 1.7 The Supplier shall provide, and shall procure that each Subcontractor shall provide, all reasonable cooperation and assistance to the Buyer, any Replacement Supplier and/or any Replacement Subcontractor 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 Subcontractor shall provide, to the Buyer or, at the direction of the Buyer, to any Replacement Supplier and/or any Replacement Subcontractor (as appropriate), in respect of each person on the Supplier's Final Supplier Personnel List who is a Transferring Supplier Employee:
 - 1.7.1 the most recent month's copy pay slip data;
 - 1.7.2 details of cumulative pay for tax and pension purposes;
 - 1.7.3 details of cumulative tax paid;
 - 1.7.4 tax code;
 - 1.7.5 details of any voluntary deductions from pay; and
 - 1.7.6 bank/building society account details for payroll purposes.

2. Staff Transfer when the contract ends

- 2.1 The Buyer 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 the relevant Contract or otherwise) resulting in the Services being undertaken by a Replacement Supplier and/or a Replacement Subcontractor. Such change in the identity of the supplier of such services may constitute a Relevant Transfer to which the Employment Regulations and/or the Acquired Rights Directive will apply. The Buyer and the Supplier agree that, as a result of the operation of the Employment Regulations, where a Relevant Transfer occurs, the contracts of employment between the Supplier and the Transferring Supplier Employees (except in relation to any contract terms disapplied through operation of regulation 10(2) of the Employment Regulations) will have effect on and from the Service Transfer Date as if originally made between the Replacement Supplier and/or a Replacement Subcontractor (as the case may be) and each such Transferring Supplier Employee.
- 2.2 The Supplier shall, and shall procure that each Subcontractor 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 Subcontractor shall perform and discharge, all its obligations in respect of all the Transferring Supplier Employees arising in respect of the period up to (and including) the Service Transfer Date (including (without limit) the payment of all remuneration, benefits, entitlements, and outgoings, all wages, accrued

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2018

but untaken holiday pay, bonuses, commissions, payments of PAYE, national insurance contributions and 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 (and including) the Service Transfer Date) and any necessary apportionments in respect of any periodic payments shall be made between: (i) the Supplier and/or the Subcontractor (as appropriate); and (ii) the Replacement Supplier and/or Replacement Subcontractor.

2.3 Subject to Paragraph 2.4, the Supplier shall indemnify the Buyer and/or the Replacement Supplier and/or any Replacement Subcontractor against any Employee Liabilities arising from or as a result of:

- 2.3.1 any act or omission of the Supplier or any Subcontractor in respect of any Transferring Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Supplier Employee whether occurring before, on or after the Service Transfer Date;
- 2.3.2 the breach or non-observance by the Supplier or any Subcontractor occurring on or before the Service Transfer Date of:
 - (a) any collective agreement applicable to the Transferring Supplier Employees; and/or
 - (b) any other custom or practice with a trade union or staff association in respect of any Transferring Supplier Employees which the Supplier or any Subcontractor is contractually bound to honour;
- 2.3.3 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 a Subcontractor to comply with any legal obligation to such trade union, body or person arising on or before the Service Transfer Date;
- 2.3.4 any proceeding, claim or demand by HMRC or other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:
 - (a) in relation to any Transferring Supplier Employee, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising on and before the Service Transfer Date; and

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2018

- (b) 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 his/her employment from the Supplier to the Buyer and/or Replacement Supplier and/or any Replacement Subcontractor, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising on or before the Service Transfer Date;
 - 2.3.5 a failure of the Supplier or any Subcontractor 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 Supplier Employees in respect of the period up to (and including) the Service Transfer Date);
 - 2.3.6 any claim made by or in respect of any person employed or formerly employed by the Supplier or any Subcontractor other than a Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List for whom it is alleged the Buyer and/or the Replacement Supplier and/or any Replacement Subcontractor may be liable by virtue of the relevant Contract and/or the Employment Regulations and/or the Acquired Rights Directive; and
 - 2.3.7 any claim made by or in respect of a Transferring Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Supplier Employee relating to any act or omission of the Supplier or any Subcontractor 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 Buyer and/or Replacement Supplier 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 an act or omission of the Replacement Supplier and/or any Replacement Subcontractor whether occurring or having its origin before, on or after the Service Transfer Date including any Employee Liabilities:
- 2.4.1 arising out of the resignation of any Transferring Supplier Employee before the Service Transfer Date on account of substantial detrimental changes to his/her working conditions proposed by the Replacement Supplier and/or any Replacement Subcontractor to occur in the period on or after the Service Transfer Date); or

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2018

- 2.4.2 arising from the Replacement Supplier's failure, and/or Replacement Subcontractor's failure, to comply with its obligations under the Employment Regulations.
 - 2.5 If any person who is not identified in the Supplier's Final Supplier Employee List claims, or it is determined in relation to any employees of the Supplier, that his/her contract of employment has been transferred from the Supplier to the Replacement Supplier and/or Replacement Subcontractor pursuant to the Employment Regulations or the Acquired Rights Directive, then:
 - 2.5.1 the Buyer shall procure that the Replacement Supplier and/or Replacement Subcontractor will, within 5 Working Days of becoming aware of that fact, notify the Buyer and the Supplier in writing; and
 - 2.5.2 the Supplier may offer (or may procure that a Subcontractor may offer) employment to such person, or take such other reasonable steps as it considered appropriate to deal the matter provided always that such steps are in compliance with Law, within 15 Working Days of receipt of notice from the Replacement Supplier and/or Replacement Subcontractor.
 - 2.6 If such offer of is accepted, or if the situation has otherwise been resolved by the Supplier or a Subcontractor, Buyer shall procure that the Replacement Supplier shall, or procure that the and/or Replacement Subcontractor shall, immediately release or procure the release the person from his/her employment or alleged employment;
 - 2.7 If after the 15 Working Day period specified in Paragraph 2.5.2 has elapsed:
 - 2.7.1 no such offer has been made:
 - 2.7.2 such offer has been made but not accepted; or
 - 2.7.3 the situation has not otherwise been resolved
- the Buyer shall advise the Replacement Supplier and/or Replacement Subcontractor (as appropriate) that it may within 5 Working Days give notice to terminate the employment or alleged employment of such person;
- 2.8 Subject to the Replacement Supplier's and/or Replacement Subcontractor 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 and subject to Paragraph 2.9 below, the Supplier will indemnify the Replacement Supplier and/or Replacement Subcontractor against all Employee Liabilities arising out of the termination of the employment of any of the Supplier's employees pursuant to the provisions of Paragraph 2.7 provided that the Replacement Supplier takes, or shall procure that the Replacement Subcontractor takes, all reasonable steps to minimise any such Employee Liabilities.
 - 2.9 The indemnity in Paragraph 2.8:
 - 2.9.1 shall not apply to:

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2018

- (a) any claim for:
 - (i) discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief; or
 - (ii) 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 Replacement Supplier and/or Replacement Subcontractor, or

- (b) any claim that the termination of employment was unfair because the Replacement Supplier and/or Replacement Subcontractor neglected to follow a fair dismissal procedure; and

2.9.2 shall apply only where the notification referred to in Paragraph 2.5.1 is made by the Replacement Supplier and/or Replacement Subcontractor 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 Subcontractor nor dismissed by the Replacement Supplier and/or Replacement Subcontractor 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 Subcontractor shall comply, with all its obligations under the Employment Regulations and shall perform and discharge, and shall procure that each Subcontractor shall perform and discharge, all its obligations in respect of any person identified in the Supplier's Final Supplier Personnel List before and on the Service Transfer Date (including the payment of all remuneration, benefits, entitlements and outgoings, all wages, accrued but untaken holiday pay, bonuses, commissions, payments of PAYE, national insurance contributions and pension contributions and 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 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:

- (b) the Supplier and/or any Subcontractor; and
- (c) the Replacement Supplier and/or the Replacement Subcontractor.

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2018

- 2.12 The Supplier shall, and shall procure that each Subcontractor shall, promptly provide the Buyer and any Replacement Supplier and/or Replacement Subcontractor, in writing such information as is necessary to enable the Buyer, the Replacement Supplier and/or Replacement Subcontractor to carry out their respective duties under regulation 13 of the Employment Regulations. The Buyer shall procure that the Replacement Supplier and/or Replacement Subcontractor, shall promptly provide to the Supplier and each Subcontractor in writing such information as is necessary to enable the Supplier and each Subcontractor to carry out their respective duties under regulation 13 of the Employment Regulations.
- 2.13 Subject to Paragraph 2.14, the Buyer shall procure that the Replacement Supplier indemnifies the Supplier on its own behalf and on behalf of any Replacement Subcontractor and its Subcontractors against any Employee Liabilities arising from or as a result of:
- 2.13.1 any act or omission of the Replacement Supplier and/or Replacement Subcontractor in respect of any Transferring Supplier Employee in the Supplier's Final Supplier Personnel List or any appropriate employee representative (as defined in the Employment Regulations) of any such Transferring Supplier Employee;
 - 2.13.2 the breach or non-observance by the Replacement Supplier and/or Replacement Subcontractor on or after the Service Transfer Date of:
 - (a) any collective agreement applicable to the Transferring Supplier Employees identified in the Supplier's Final Supplier Personnel List; and/or
 - (b) any custom or practice in respect of any Transferring Supplier Employees identified in the Supplier's Final Supplier Personnel List which the Replacement Supplier and/or Replacement Subcontractor is contractually bound to honour;
 - 2.13.3 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 and/or Replacement Subcontractor to comply with any legal obligation to such trade union, body or person arising on or after the Service Transfer Date;
 - 2.13.4 any proposal by the Replacement Supplier and/or Replacement Subcontractor 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 Subcontractor (as the case may be) on the Service Transfer Date, or to change the terms and conditions of employment or

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2018

- 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;
- 2.13.5 any statement communicated to or action undertaken by the Replacement Supplier or Replacement Subcontractor to, or 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;
- 2.13.6 any proceeding, claim or demand by HMRC or other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:
- (a) 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 other statutory authority relates to financial obligations arising after the Service Transfer Date; and
 - (b) 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 his/her employment from the Supplier or Subcontractor, to the Replacement Supplier or Replacement Subcontractor to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising after the Service Transfer Date;
- 2.13.7 a failure of the Replacement Supplier or Replacement Subcontractor 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 Supplier Employees identified in the Supplier's Final Supplier Personnel List in respect of the period from (and including) the Service Transfer Date; and
- 2.13.8 any claim made by or in respect of a Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List or any appropriate employee representative (as defined in the Employment Regulations) of any such Transferring Supplier Employee relating to any act or omission of the Replacement

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2018

Supplier or Replacement Subcontractor 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 an act or omission of the Supplier and/or any Subcontractor (as applicable) 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 and/or any Subcontractor (as applicable) to comply with its obligations under the Employment Regulations.

Call-Off Schedule 3 (Continuous Improvement)

Call-Off Ref:

Crown Copyright 2018

Call-Off Schedule 3 (Continuous Improvement)

1. Buyer's Rights

- 1.1 This Schedule shall apply only when so specified by a Buyer that has undertaken a Further Competition. The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), the Buyer may give CCS the right to enforce the Buyer's rights under this Schedule.

2. Supplier's Obligations

- 2.1 The Supplier shall have an ongoing obligation throughout the Contract Period, to identify new or potential improvements to the provision of the Deliverables in accordance with this Call Off Schedule 3 with a view to reducing the Buyer's costs (including the Call-Off Contract Charges) and/or improving the quality and efficiency of the Deliverables and their supply to the Buyer. As part of this obligation the Supplier shall identify and report to the Buyer once every twelve (12) months regarding:

- 2.1.1 the emergence of new and evolving relevant technologies which could improve the ICT Environment and/or the provision of the Deliverables, and those technological advances potentially available to the Supplier and the Buyer which the Parties may wish to adopt;
- 2.1.2 new or potential improvements to the Deliverables or the provision of the Deliverables including in respect of the quality, responsiveness, procedures, benchmarking methods, ways of performing the Services and customer support services in relation to the Deliverables;
- 2.1.3 changes in business processes and working practices that would enable the Deliverables to be provided at lower cost and/or with greater benefits to the Buyer;
- 2.1.4 changes to the ICT Environment, business processes and working practices that would enable reductions in the total energy consumed in the provision of the Deliverables;
- 2.1.5 improvements which the Supplier uses or is planning to use with its other customers;
- 2.1.6 proposals as to how any investment required for continuous improvement could be shared with other customers of the Supplier;
- 2.1.7 a zero usage report to identify opportunities for cost avoidance;
- 2.1.8 measuring and reducing the sustainability impacts of the Supplier's operations and supply-chains relating to the

Framework Ref: RM6116

Project Version: v1.1

Model Version: v3.0

Call-Off Schedule 3 (Continuous Improvement)

Call-Off Ref:

Crown Copyright 2018

Deliverables, and identifying opportunities to assist the Buyer in meeting their sustainability objectives;

- 2.2 The Supplier must adopt a policy of continuous improvement in relation to the Deliverables, which must include regular reviews with the Buyer of the Deliverables and the way it provides them, with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables. The Supplier and the Buyer must provide each other with any information relevant to meeting this objective.
- 2.3 The initial Continuous Improvement Plan for the first (1st) Contract Year shall be submitted by the Supplier to the Buyer for Approval within one hundred (100) Working Days of the first Order or six (6) Months following the Start Date, whichever is earlier.
- 2.4 The Buyer shall notify the Supplier of its Approval or rejection of the proposed Continuous Improvement Plan or any updates to it within twenty (20) Working Days of receipt. If it is rejected then the Supplier shall, within ten (10) Working Days of receipt of notice of rejection, submit a revised Continuous Improvement Plan reflecting the changes required. Once Approved, it becomes the Continuous Improvement Plan for the purposes of this Contract.
- 2.5 The Supplier must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Supplier shall provide any further information as requested.
- 2.6 If the Buyer wishes to incorporate any improvement identified by the Supplier into this Contract, including any impact on the Charges declared by the Supplier as part of that improvement, it must request a Variation in accordance with the Variation Procedure and the Supplier must implement such Variation at no additional cost to the Buyer or CCS.
- 2.7 Once the first Continuous Improvement Plan has been Approved in accordance with Paragraph 2.5:
 - 2.7.1 the Supplier shall use all reasonable endeavours to implement any agreed deliverables in accordance with the Continuous Improvement Plan; and
 - 2.7.2 the Parties agree to meet as soon as reasonably possible following the start of each quarter (or as otherwise agreed between the Parties) to review the Supplier's progress against the Continuous Improvement Plan.
- 2.8 The Supplier shall update the Continuous Improvement Plan as and when required but at least once every Contract Year (after the first (1st) Contract Year) in accordance with the procedure and timescales set out in Paragraph 2.3.
- 2.9 All costs relating to the compilation or updating of the Continuous Improvement Plan and the costs arising from any improvement made pursuant to it and the costs of implementing any improvement, shall have no effect on and are included in the Charges.

Call-Off Schedule 3 (Continuous Improvement)

Call-Off Ref:

Crown Copyright 2018

- 2.10 Should the Supplier's costs in providing the Deliverables to the Buyer be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Buyer by way of a consequential and immediate reduction in the Charges for the Deliverables.
- 2.11 At any time during the Contract Period of the Call-Off Contract, the Supplier may make a proposal for gainshare. If the Buyer deems gainshare to be applicable then the Supplier shall update the Continuous Improvement Plan so as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio.
- 2.12 Notwithstanding anything to the contrary in this Call-Off Contract, the Parties may not change or improve the Deliverables in any way which adversely affects or may adversely affect any relevant PSN Standards or HSCN obligations and processes.

Call-Off Schedule 5 (Pricing Details)

Call-Off Ref:

Crown Copyright 2018

Call-Off Schedule 5 (Pricing Details)

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN****Public Sector**

- c) Call-Off Schedule 9 (Security) - Security Management Plan in accordance with Call-Off Schedule 9. The Buyer hereby acknowledges and agrees that the Supplier's Security Management Plan is incorporated in Part A of Call-Off Schedule 9 . . By entering into a Call-Off Contract the Buyer acknowledges and agrees:
 - i) the Supplier has prepared and delivered the Security Management Plan to the Buyer; and
 - ii) the Buyer has approved the Security Management Plan, in accordance with Call-Off Schedule 9 (Security) Part A: Short Form Security Requirements.

8. Service Description and Price Card

8.1. Primary Services

IP-VPN is a secure, private Wide Area Network (WAN) service which supports data, voice, and video traffic virtually over a shared packet network. IP-VPN can be used for point to multi-point or “any to any” wide area communications. IP-VPN is based on a Multi-Protocol Label Switching (MPLS) core, transporting IP traffic.

The service enables the Buyer to establish a private wide area network to underpin critical communications. An IP Virtual Private Network (VPN) is built and configured between various nominated Buyer Sites, which are connected to the Vodafone IP-MPLS Network using a range of site topologies and network access methods to meet availability and performance requirements.

The IP-VPN Service provides the Buyer with data connectivity between Buyer sites and enables the sharing of data services between each of the connected sites. If the Buyer requires any technical information beyond the scope of this Service Offer in relation to the Vodafone IP-VPN service, a technical specification can be made available on request by contacting your Vodafone account manager, or frameworks_team@vodafone.com.

- a) The main service components of the IP-VPN service are:
 - i) Access circuit – this connects a Buyer Site to a port on Vodafone's MSP network. The port bandwidth can be throttled allowing the Buyer to pay only for the service bandwidth which it needs. Backup and Resilience options are also supported.
 - ii) Class of Service (QoS) – the IP-VPN service supports the standard six (6) traffic differentiation classes on all Ethernet access types (not available on ADSL16 and FTTC Elevated 40/10). These are summarised in the below table
 - iii) Buyer Premise Equipment (BPE) (i.e. Router) – The service can be provided on a wires-only basis or inclusive of managed Buyer Premise Equipment router hardware
 - A) If the Vodafone Supplied Router becomes unsupported by the manufacturer, Vodafone may replace the Vodafone Supplied Router with an equivalent supported router at Vodafone's discretion.
 - B) BPE are specified and tested up to a recommended maximum throughput. The Buyer must specify a BPE who's maximum throughput is higher than the service speed called off.
 - iv) Service and support on a 24x7x365 basis with proactive monitoring (Severity Level 1-2 Incidents) and 24/7 Incident Management; including interface down, BGP routing failure, bouncing interfaces, unreachable device.
- b) Optional features of the IP-VPN service are:
 - i) Network Based Internet Access and network-based Firewall including Secure Network Gateway – access to the Internet from within the network securely

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN****Public Sector**

- ii) Secure Internet Site Access – a remote access connectivity to your IP-VPN network for users or 3rd parties working at a specific remote location
- iii) Cloud Connect – access to centralised cloud-based applications from within your IP-VPN network hosted within cloud providers such as Amazon, Google, and Microsoft.

Quality of Service classes and recommended use.

The IP-VPN service supports differentiation of traffic across the network by the application of Quality of Service. The six classes available are shown below. A service can consist of a single class; two classes or more or all classes on the same site connection and network as befits the Buyer requirements

Note: not all Class of Service levels are available where access uses DSL, GPON or SISA.

The VPN port bandwidth Annual Recurring Charge defined under this Service Offer is for Default class bandwidth. Charges for other traffic classes are detailed section 8.15 and are in addition to the VPN port bandwidth Annual Recurring Charge.

Class of Service	Description	Typical Applications	Application Characteristics
Premium	The highest-level CoS, prioritised over all other traffic.	Voice, Video Conferencing	Real time, business critical, designed for voice.
Enhanced 1 Enhanced 2 Enhanced 3	Three Enhanced classes to enable separation of different types of critical traffic.	Enterprise applications such as Citrix, Oracle, SAP. Financial transactions, streamed video. Allocating applications to an Enhanced CoS can protect them from high-bandwidth, low-priority traffic such as FTP and HTTP downloads.	Important, interactive, less sensitive to jitter but still delay sensitive.
Standard		Email, web browsing, FTP, HTTP downloads.	Not real time or interactive. Not sensitive to jitter or delay but more important than reasonable efforts traffic (Default Class)
Default	The lowest-level CoS.	Email, web browsing, FTP, HTTP downloads.	Not real time or interactive. Not sensitive to jitter or delay

Additional default class traffic is selected by choosing the relevant VPN port bandwidth. Standard class is charged at the same rate as default class and where required must be stated at time of order.

- c) The Charges payable in respect of this Service are set out in the Price Card below.

The Charges for single circuit are made up of:

- i) Set up/Installations Fee (One Off)
- ii) Annual recurring charges (billed either monthly or annually)
- iii) Modification Charges (where requested by the Buyer);
- iv) Professional Services (if applicable)
- v) Support Service (if applicable)
- vi) Optional Managed Router (this is where Vodafone will provide proactive management and maintenance of the Vodafone provided router)

- d) All pricing is based on either a 12-month, 24-month, or 36-month initial period.

RM6116 Network Services 3

Lot 1a – Inter site Connectivity/Data Access Services

Vodafone IP-VPN

Public Sector



- e) Buyer Premise Equipment (BPE) – where optional managed routers are chosen by the Buyer, the routers will be installed, configured, managed, and maintained by Vodafone. There are two types of BPE a Buyer can purchase;
 - i) Standard – Router hardware capable of supporting the requested VPN (port) throughput bandwidth as measured using an IMIX traffic profile.
 - ii) Premium – Router hardware capable of offering a higher service performance and supporting upgrades in VPN (port) bandwidth without a change in router hardware. Premium router hardware shall be capable of supporting the maximum VPN (port) bandwidth possible on the chosen access connectivity based on a IMIX traffic profile. Premium router hardware should be selected where there is a requirement for a small average 64 Byte packet size (such as for large IP Voice traffic usage)
- f) Enhanced Network Performance Service reporting – where ordered, reporting options are available which give greater visibility of service performance adding Latency, Jitter and Packet loss visibility between selected Buyer sites. Vodafone IP-VPN Online Performance Reporting (OPR) provides you the visibility required to plan, deploy, ensure, troubleshoot, and optimise complex WAN environments and applications. It empowers your IT organisation with the real-time technical insight and business relevant performance metrics needed to guarantee end-user satisfaction and productivity. Capability offered includes:
 - i) Global Dashboard With a Summary of Site Inventory
 - ii) Detailed Site Inventory
 - iii) Planned Outage notifications Dashboard Network Performance Reporting

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services**

Vodafone IP-VPN

Public Sector

**IP-VPN 2 Year Pricing - Single Circuit Service**

All pricing excludes VAT

Site	Primary / Secondary	Postcode	Service Speed / Bandwidth	Access Type	CoS - Standard / Enhanced / Premium or ADSL/SFA Profile Number	Router	One off Charges - NRC	Monthly Charge (£) MRC	Annual Charge (£) ARC

SNG

Type	One off Charges - NRC	Monthly Charge (£) MRC	Annual Charge (£) ARC

Microsoft Cloud Connect

Type	One off Charges - NRC	Monthly Charge (£) MRC	Annual Charge (£) ARC

TSSM

Type	One off Charges - NRC	Monthly Charge (£) MRC	Annual Charge (£) ARC due in advance

RM6116 Network Services 3

Lot 1a – Inter site Connectivity

Vodafone IP-VPN

Public Sector



g) Enhanced Class of Service Pricing (CoS)

Enhanced Class of Service allows for prioritisation of delay-sensitive traffic through the implementation of traffic classification (the 'marking of traffic') at the network edge for carriage across the service.

- Class of Service (COS) is priced based on the percentage of Standard VPN Port Bandwidth required as Enhanced or Premium COS.
- Use the Matrix to select the COS Price. All Prices are ARC.
- Select Standard VPN Port in the Vertical Column and scroll Horizontally to the required Premium COS Bandwidth.
- Premium and Enhanced COS Prices are in addition to Standard VPN Port Pricing.
- All Prices are ARC.

RM6116 Network Services 3

Lot 1a – Inter site Connectivity/Data Access Services

Vodafone IP-VPN

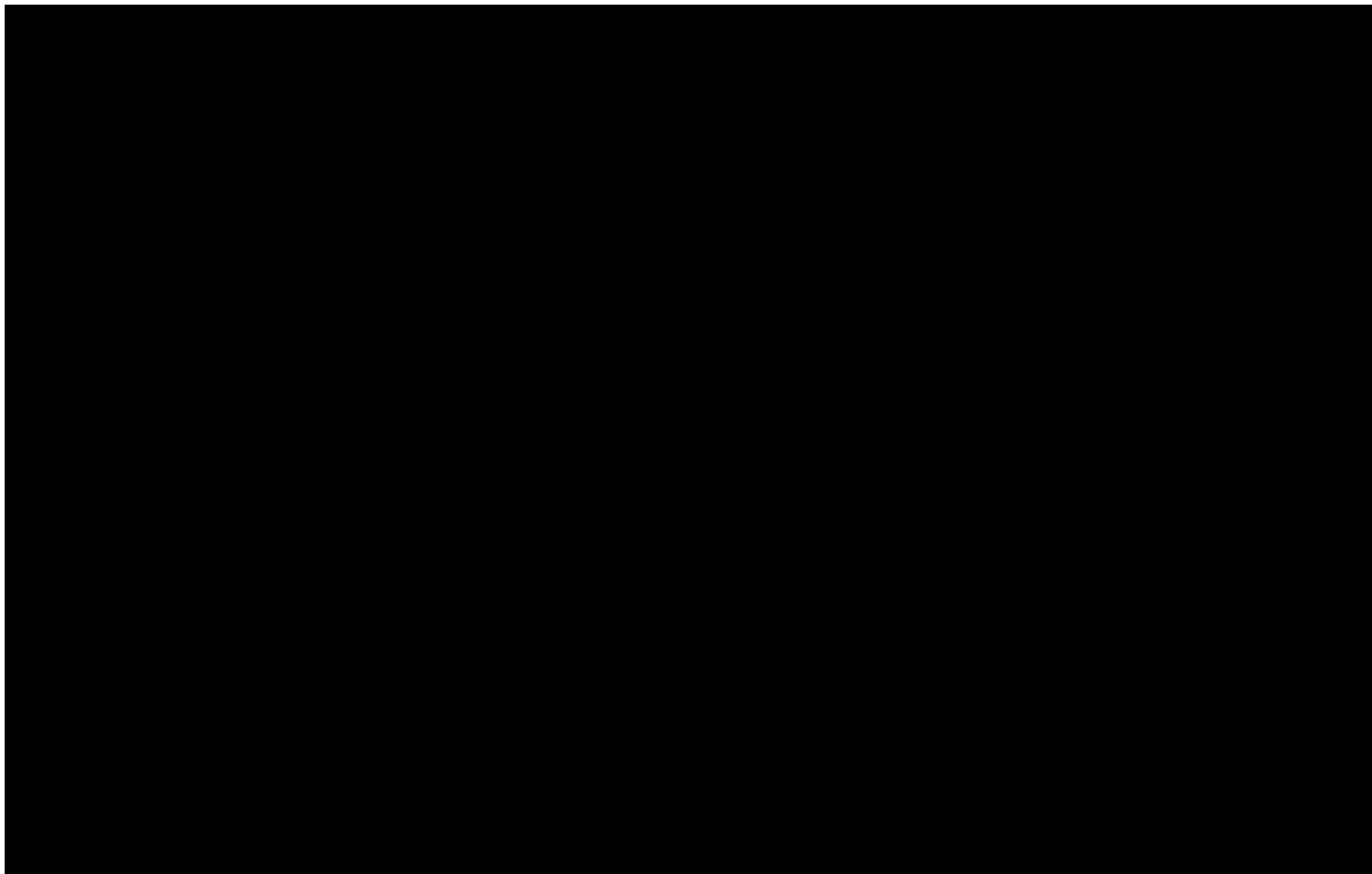
Public Sector



h) Premium Class of Services (CoS)

Premium Class of Service allows for prioritisation of delay-sensitive traffic through the implementation of traffic classification (the 'marking of traffic') at the network edge for carriage across the service.

- Class of Service (COS) is priced based on the percentage of Standard VPN Port Bandwidth required as Enhanced or Premium COS
- Use the Matrix to select the COS Price. All Prices are ARC
- Select Standard VPN Port in the Vertical Column and scroll Horizontally to the required Premium COS Bandwidth
- Premium and Enhanced COS Prices are in addition to Standard VPN Port Pricing.



i) Cloud Connect Pricing – 12 Month

Cloud Connect provides private connectivity to Cloud Provider Data Centre directly from the IP-VPN Network, for improved security, performance and availability compared to using the public Internet. Cloud Connect provides the following capabilities:

- Consistent, committed bandwidth at rates from 50Mbps to 1Gbps allowing Network capacity to scale as required.
- Flexible contract duration from one month to sixty months.
- Includes dual access from two PEs to a Cloud Provider Data Centre for high availability.
- Secure private connections ensure the Buyer's traffic is segregated.
- Authorisation of connections maintains the confidentiality and integrity of information.
- Connectivity to Cloud Provider Data Centre locations in different regions reduces latency and aids compliance with data residency and data sovereignty requirements.
- Managed service including ordering, support, escalations, reporting and ticketing (as for IP-VPN).

RM6116 Network Services 3

Lot 1a – Inter site Connectivity/Data Access Services

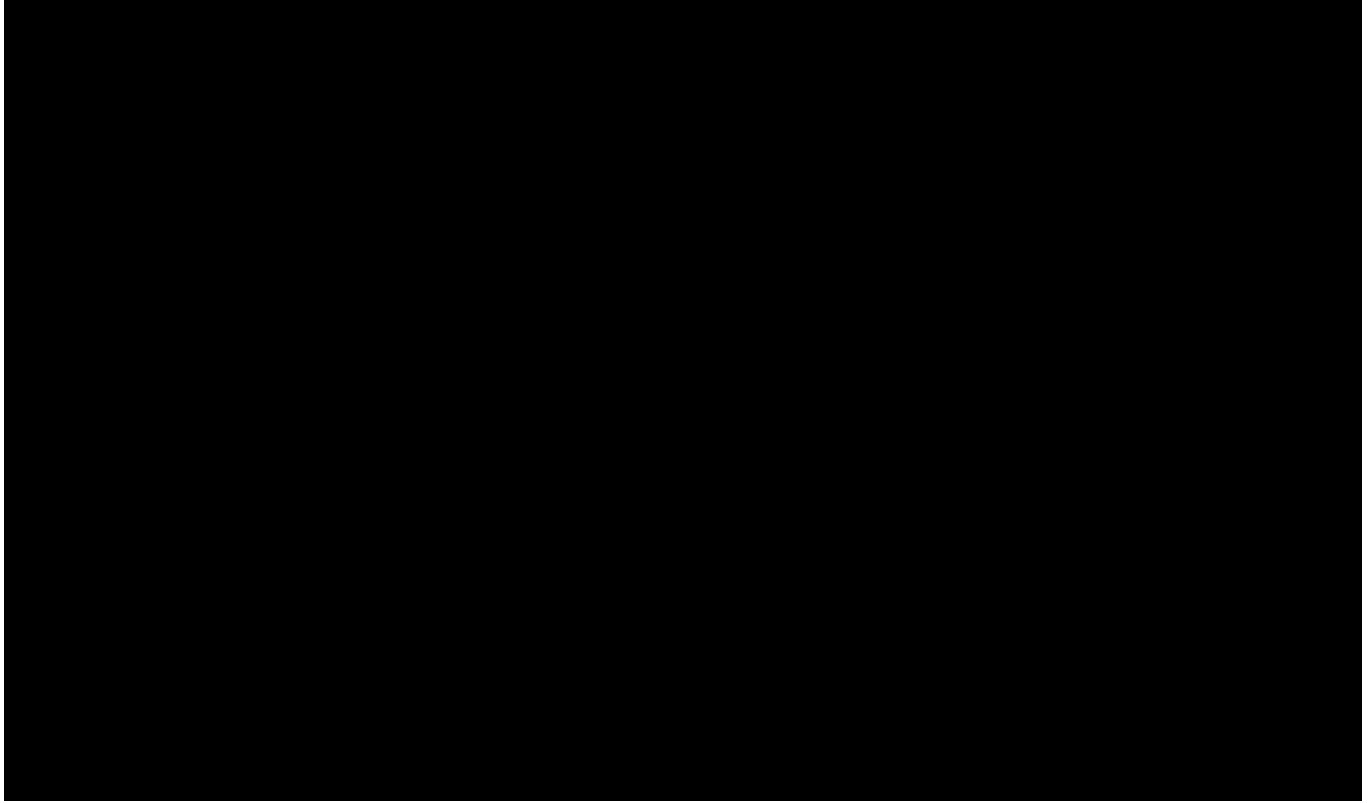
Vodafone IP-VPN

Public Sector



8.2. Technology, Equipment and Solutions

Additional Services



RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN****Public Sector****Enhanced Network Based Internet Access (NBIA)**

Enhanced NBIA provides Users at any Buyer Site on a Buyer's IP-VPN with a central public Internet gateway facility. The Enhanced NBIA service by default comes with a basic ruleset to allow outbound but restrict inbound access. This default firewall will provide the minimum level of security and suits simple web browsing use cases for Enhanced NBIA. For greater granularity of control, and to allow additional features such as application reporting, then Vodafone can provide a range of Firewall options that increase in functionality to a fully managed, premium, firewall option.

Buyer's use of Enhanced NBIA is limited to the following countries at time of contracting:

Vodafone Licenced Countries		
Austria	Hong Kong	Portugal
Australia	Hungary	Russia
Belgium	Italy	Singapore
Canada	Ireland (Republic of)	South Korea
Czech Republic	Japan	Spain
Bulgaria	Luxembourg	Sweden
Denmark	Malaysia	Switzerland
Finland	Mexico	Ukraine
France	Netherlands	UK
Germany	Norway	USA

Secure Network Gateway:

SNG is ordered with Enhanced NBIA. Buyer may order a range of firewall and security features under the Standard and Premium packages set out below. SNG Service includes a network-based firewall facility. If ordered, Vodafone will consult with Buyer to capture preferred security rules and configuration requirements.

(i) The following Standard and Premium feature sets are available:

Items	Standard	Premium
Inbound/outbound ruleset	Up to 50	Up to 1000
Application reporting	Yes –	Yes -
Firewall event/logs	6-month retention	12-month retention
Reports frequency	weekly/monthly	Daily/weekly/monthly

(ii) Additional options for intrusion Detection and Prevention are set out below:

Items	Standard	Premium
Policy protection	Default	Customisable
Threat detection via SSL	No	Yes
Anomaly based detection	No	Yes - with tuning support
NIDs/NIPs events/logs	6-month retention	12-month retention
Reports frequency	weekly/monthly	Daily/weekly/monthly

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services**

Vodafone IP-VPN

Public Sector



✕ = Not Available ✓ = Included in Package ● = Optional Add-on (Additional Charge)		Firewall Type (Package)		
Description	Features	Default (Enhanced NBIA Only)	Standard Firewall	Premium Firewall
Enhanced NBIA Only Default ruleset for Enhanced NBIA – allowing all outbound access with PAT to single public address Fully Managed Enhanced NBIA with Firewall service to support outbound & inbound security policies.	Ruleset allowing all outbound traffic Ruleset preventing all inbound traffic	✓	✕	✕
	Inbound and outbound rulesets and	✕	✓ Up to 50	✓ Up to 1000
	Change Management through Vodafone service desk	✕	✓	✓
	Firewall event/logs for downloading within Vodafone portal (6-month retention)	✕	✓ 6 months log retention	✓ 12 months log retention
	Firewall reports - Ability to view, & download (or email) reports via Oneportal	✕	✓	✓
	DMZ deployment for public facing applications (recommended for inbound access from internet)	✕	● Optional Add-on	● Optional Add-on
	External Syslog feed (for 3rd party)	✕	● Optional Add-on	● Optional Add-on
	Integration with Buyer AD/Directory for user aware policies. Up to 5 AD servers/domains	✕	✕	✓
	Firewall based traffic shaping for application prioritisation, including bandwidth limiting of applications Up to 3 traffic shaping profiles	✕	✕	● Optional Add-on



11/11/2016

RM6116 Network Services 2



Lot 1a – Inter site Connectivity / Data Access Services

Vodafone Dedicated Internet Access

Public Sector

- i) the Supplier has prepared and delivered the Security Management Plan (published as set out above) to the Buyer; and
- ii) the Buyer has approved the Security Management Plan, in accordance with Call-Off Schedule 9 (Security) Part A: Short Form Security Requirements.

8. Service Description and Price Card

8.1. Primary Services

The Vodafone Dedicated Internet Access Services provide Buyer with symmetrical access to the public internet either over dedicated access bearers, shared access bearers, or directly to Vodafone's IP-VPN network. The Service is provided using the Global Vodafone IP Backbone or a combination of the Global Vodafone IP Backbone and the Vodafone Global IP-MPLS Networks. The term "Service" or "Services" in these Service Specific Terms means the Internet Access Services (as further detailed in the Service Specification).

Wires Only – Buyers have the option of a 12, 24 or 36-month term.

Dedicated Symmetrical Access Circuits - Buyers do not have to share their bandwidth with anyone else. Buyers receive all the bandwidth that they are paying for. Symmetrical circuits allow Buyers to utilise the full available bandwidth for either upstream or downstream traffic. There are no restrictions on monthly usage or additional charges for large files.

Choice of access connectivity - Fibre-based Ethernet, connections at any of the standard 100Mbps, 1000Mbps or 10Gbps speeds. The Dedicated Internet Access Service can be provided at a range of lower 'throttled' speeds, so Buyers only pay for the bandwidth provided. The Buyer can take the higher bandwidth when the Buyer's requirements change. Buyers are able to order the following committed bandwidth combinations;

Buyer Premise Equipment (BPE) (i.e. Routers) – where ordered these will be installed, configured, managed and maintained by Vodafone. BPE and other devices inherit the physical controls of the Buyer environment in which they are installed. In addition to these physical controls, additional controls are deployed to help mitigate the risks associated with power (feeds, power distribution units, UPS or equivalent backup generators) and cabling security (e.g. change management, dual routing, cable labelling, tidy & careful cabling to documented standards (e.g. avoids bends, kinks), use of ducting and where possible enclosed metal or clear conduit. There are three types of BPE a Buyer can rent;

- a) Low – Router hardware capable of supporting the requested VPN (port) throughput bandwidth as measured using an IMIX traffic profile
- b) Medium – Router hardware capable of supporting the requested VPN (port) throughput bandwidth as detailed in the router pricing section.
- c) High – Router hardware capable of offering a higher service performance and supporting upgrades in VPN (port) bandwidth without a change in router hardware. Premium router hardware shall be capable of supporting the maximum VPN (port) bandwidth possible on the chosen access connectivity based on a IMIX traffic profile. Premium router hardware should be selected where there is a requirement for a small average 64 Byte packet size (such as for large IP Voice traffic usage)

Access Circuit Bandwidth	Committed Service Bandwidths	Committed + Burst Service Bandwidths (Global IP-MPLS Access types only)	Access Technology	Interface (Buyer Provided Router)
100Mbps	10, 15, 20, 30, 40, 50, 60, 70, 80, 90, 100Mbps	10Mbps burst to 20Mbps 20Mbps burst to 40Mbps 50Mbps burst to 100Mbps	Ethernet	RJ45



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

[Redacted]

[Redacted]

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

[Redacted]

[Redacted]

Performance Reporting per Site

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

Internet Features

- Public IP Addresses

[Redacted]

[Redacted]

[Redacted]



Vodafone Dedicated Internet Access

Public Sector

8.2. Ancillary Services

Ancillary Charges associated with services provided by a third party /OLO

Unless otherwise agreed and stated in the Buyer's Call-Off Contract, the Buyer will be liable for any additional costs charged to Vodafone by third parties in connection with the provision of the Services. Such Charges include but are not limited to the following:

[illegible]

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector****Professional Services**

Vodafone offer a range of professional services including technical consultancy, project management and on-site service management.

Charges	
	Maximum daily rates excluding expenses
Consultants	
Junior Consultant	
Consultant	
Senior Consultant	
Principal Consultant	
Partner/ Director	
Contractors / IT Specialists	
Senior Analyst/ Team Leader	
Systems Analyst & Designers	
Analyst/ Programmers	
Application Programmers	
System Programmers	
Database Administrators	
Network Administrators	
Capacity Planners	
Configuration Managers	
IT Trainers	
Documentation Specialists	
Project Administrators	

9. Key Sub-Contractors

- Openreach Limited
 - Kelvin House, 123 Judd Street, London, United Kingdom, WC1H 9NP
 - 10690039
- Virgin Media Limited
 - Media House, Bartley Wood Business Park, Hook, Hampshire, RG27 9UP
 - 02591237
- CityFibre Limited
 - 15 Bedford Street, London, England, WC2E 9HE
 - 09759465



RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector

7. Mandatory Schedules

- 7.1 In accordance with the Supplier's obligations under any Call-Off Contract, Vodafone has developed and will maintain the following reports and plans, which are available to view, download, print or save, on Vodafone's Public Sector Portal. By entering into a Call-Off Contract, the Buyer confirms that it accepts the following reports and plans as is, with no alteration:

- (a) Call-Off Schedule 1 (Transparency Reports) - Transparency Report in accordance with clause 1, of Call-Off Schedule 1.
- (b) Call-Off Schedule 8 (Business Continuity and Disaster Recovery) – Business Continuity and Disaster recovery Plan in accordance with Clause 1, of Call-Off Schedule 8.
- (c) Call-Off Schedule 9 (Security) -Security Management Plan in accordance with Clause 4, of Call-Off Schedule 9.

The Security Management Plan for any Deliverables purchased under this Service Offer shall be the Supplier's Security Management Plan published on Vodafone's Public Sector Portal. By entering into a Call-Off Contract the Buyer acknowledges and agrees:

- (i) The Supplier has prepared and delivered the Security Management Plan (published as set out above) to the Buyer; and
- (ii) The Buyer has approved the Security Management Plan, in accordance with paragraphs 4.3.1 and 4.3.2 of Call-Off Schedule 9 (Security) Part A: Short Form Security Requirements.

8. Service Description and Price Card

Vodafone's wired and wireless Local Area Network (LAN) solution give users secure and reliable access to business systems and resources from any device.

A local area network (LAN) is a network that interconnects computers within a limited area such as a home, office building or warehouse. A LAN will interconnect to a Wide Area Network (WAN) or the internet by an external fixed communications line.

Ethernet and Wi-Fi are the two most common transmission technologies in use for local area networks.

Vodafone's technology partner of choice is Cisco (including Meraki), who are recognised as a market leader in wired and wireless LAN technology.

Under this Service Offer, Buyers may take the hardware devices that form the LAN and in addition may take one of the incremental Service Wraps.

8.1 Primary Services

The Services shall be based on the delivery of solutions from a single vendor, Cisco Systems Limited, and consist of:

- LAN Design and Build
- Maintained LAN (including Wi-Fi) - detailed as Maintained in the price card below.
- Monitored ("Monitoring") LAN (including Wi-Fi) – detailed as Monitoring in the price card below.
- Managed ("Management") LAN (including Wi-Fi) - detailed as Management in the price card below.

The types of equipment supported shall include but not limited to:

- Wireless access points
- Meraki access points
- Meraki or Cisco switches



RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector

Each device requires a licence to operate. In the case of the security appliance, there are two types. If the Buyer requires Antivirus, Anti Phishing or Content filtering then the Buyer will need to select the Advanced Security & Support Licence, if not then select the Enterprise & Support Licence.

LAN Design and Build

The LAN Design and Build Service shall include professional services to provide local connectivity services at a single site, multiple sites in the same locale, campus sites, and metropolitan area sites, enabling an end user/end user device to connect and consume a locally hosted service.

Maintained LAN

The Maintained LAN Service shall provide remote and onsite support for LAN and WLAN equipment, including fault reporting and service restoration activities. The Service can be applied at a single site, multiple sites in the same locale, campus sites, and metropolitan area sites for the ongoing support of LAN and Wireless LAN equipment that enables an end user/end user device to connect and consume a locally hosted service.

The Buyer shall have the option for the Maintained LAN Service to provide support cover for specific items of equipment in their infrastructure or for the entire LAN/WLAN infrastructure. Bronze Maintenance is offered as part of the RM6116 Standard Service Offer.

Service level	Restore SLA
Gold	5hr
Silver	8hr
Bronze	24hr

Monitored LAN

The Monitored LAN Service shall provide 24x7 remote monitoring of LAN and WLAN equipment. The Service can be provided at a single site, multiple sites in the same locale, campus sites, and metropolitan area sites. The Buyer shall have the option for the Service to provide cover for specific items of equipment in their infrastructure or for the entire LAN/WLAN infrastructure.

This Service is only available when taken in conjunction with the Maintained LAN Service.

The Service shall continually monitor designated equipment on the Buyers LAN/WLAN infrastructure to identify service defects, incidents, and alarms and shall initiate a fault response, notifying the appropriate Vodafone resolver group and the Buyer's nominated representative of such an occurrence. Faults and incidents shall be progressed for resolution by the Vodafone Help Desk to the agreed Service Maintenance Levels.

Managed LAN

The Managed LAN Service provides 24x7 management of LAN and WLAN equipment. The Service can be provided at a single site, multiple sites in the same locale, campus sites and metropolitan area sites. The Buyer shall have the option for the Service to provide cover for specific items of equipment in their infrastructure or for the entire LAN/WLAN infrastructure.

This Service is only available when taken in conjunction with the Maintained and Monitored LAN Services.

The Managed LAN Service provides 'day-to-day' support for such activities as Moves, Adds and Changes (MACs). Vodafone shall take responsibility for the overall health of the network, including equipment software revision levels, change and configuration management and capacity planning.



RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector

Managed wi-fi:

Vodafone provides the Managed Wi-Fi Service in conjunction with Cisco Meraki, LLC (a member of the Cisco Systems, Inc. group of companies) ("Cisco Meraki"). The Managed Wi-Fi Service provides Customer with wireless access points within Customer's premises and includes (i) 'out of band cloud management' where user traffic is separated from wireless access management traffic, (ii) a web-based dashboard giving Customer visibility into its network, devices and applications; (iii) access to location based analytics information and an API that allows analytics information to be shared with Customer systems.

The Managed Wi-Fi Service is delivered by Cisco Meraki will provide certain components of the Service to Buyer as follows:

- (a) Proactive Monitoring via the Cisco Meraki Portal/Dashboard.
 - (i) To deliver monitored and managed service for Managed Wi-Fi, Vodafone will use the Cisco Meraki Dashboard (Dashboard) to monitor the status of devices, manage deployment of devices and set granular user, device and application policies. This system will also be used to diagnose the cause of incidents and to make changes as requested by Buyer.
 - (ii) Vodafone will provide Buyer with access to the dashboard which allows Buyer to monitor its devices over the Internet and provides Buyer with organization-wide reporting information including license status, device counts and network health, including whether devices are alerting or offline.
- (b) Access to the Dashboard.
 - (i) Access to the Dashboard is dependent on the services that Buyer purchases.
 - (ii) Buyers who purchase devices without support or purchase the Monitored or Maintained variant of the Wi-Fi Service will receive full access (Read/Write) to the Portal.
 - (iii) Buyers who purchase devices with the Managed variant of the Wi-Fi Service will be granted limited access to the dashboard. This will exclude the capability for Buyer to configure the devices under support.

Pricing

Pricing for the Service consists of both one-off and annual recurring charges. The total charges for the Service are dependent on a number of factors specific to Buyer requirements as set out in the Order Form.

- **One-Off Charges** consist of the Charges for equipment purchased (including licences), installation and survey services, and any subsequent licence charges applicable (in the event of a licence expiry).
- **Annual Recurring charges** consist of the sum of the Service Wraps selected from the options below:

Maintained:	The Maintained pricing is based on the Buyer's physical estate, including the chassis, modules, interfaces and software.
Monitored:	The Monitored pricing is based on a flat rate per device.
Managed:	The Managed pricing is based on a flat rate per device.

- All prices are quoted in £GBP and exclusive of sales taxes.
- Pricing is for the supported products as detailed in the Price Card.

[Redacted]

[Redacted]



[Redacted]

[Redacted]

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

[Redacted]

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

[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
LAN Monitoring	[Redacted]	[Redacted]	[Redacted]
LAN Management	[Redacted]	[Redacted]	[Redacted]
<u>Totals ex VAT</u>	[Redacted]	[Redacted]	[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[illegible]

(a) [REDACTED]

(i) [REDACTED]

_____, _____, _____



(b) Site Visits By Vodafone

- (i) Additional site visits requested by the Buyer or abortive site visits will be charged as per the following table;

Ancillary Charge per visit	Description	Working Hours	Out of Normal Working Hours A (any time outside of normal Working Hours on Monday to Friday and including any time on Saturday but excluding any time within Out of Normal Working Hours B)	Out of Normal Working Hours B (any time on a Sunday or Public Holiday in the UK)
Site Visit	Buyer Site Visit required or requested (a Site Visit not identified in the Call-Off Contract)			
Cancelled Site Visit	Buyer caused cancellation of engineering Site Visit Note: No Charge if cancelled more than 48 hours before the scheduled appointment	Within 24hrs of Site Visit = full aborted Site Visit charge Between 24 and 48hrs of Site Visit = 50% of aborted Site Visit charge		

(c) Professional Services

Vodafone a range of professional services including technical consultancy, project management and on-site service management.

Charges		
	Maximum daily rates excluding expenses	
Consultants		
Junior Consultant	£	

Lot 2a - Intra Site Connectivity

Public Sector

[illegible]

- Cisco Systems Limited
 - 9-11 New Square, Bedford Lakes, Feltham, Middlesex, TW14 8HA
 - 02558939
- Maintel Limited
 - 95 Rivers Apartment, Cannon Road, London, N17 8FE
 - 03034803

The following definitions are applicable to this Service Offer:

Acknowledge	a confirmation given to Buyer that a particular request or Incident raised is valid and the provision to Buyer of a unique reference for it. "Acknowledge" shall be construed accordingly.
Agreement	Means the Call-Off Contract, Standard Service Offer and any other applicable document required for the purchase of the Service.
Applicable Law	law, regulation, binding code of practice, rule or requirement of any relevant government or governmental agency, professional or regulatory authority, sanctions (economic trade and financial sanctions laws, regulations, embargoes or restrictive measures administered), trade or export control laws each as relevant to (i) Vodafone in the provision of the Services and/or (ii) Buyer in the receipt of the Services or the carrying out of its business.
AUP	Vodafone's acceptable use policy available on request.
Available Services	The Services available from particular Helpdesks.
Buyer's Service Desk	is the service desk provided by Buyer which will be the initial point of contact between Vodafone and Buyer.
Buyer Site	as the context permits a Buyer's premises (either owned by Buyer or a third party) which Vodafone needs to access in order to deliver or install Equipment and/or to provide the Services or the location where the Services are to be provided, as set out in the Call-Off Contract.
BPE (Buyer premises equipment)	Fixed Equipment on Buyer Site.
BMI	a "Buyer major incident", being the highest category of Impact for an Incident resulting in significant disruption to the business of Buyer.

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

1. Definitions

- 1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

“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: <ul style="list-style-type: none"> (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;
“Appropriate Authority” or “Appropriate Authorities”	means the Buyer and the Cabinet Office Markets and Suppliers Team or, where the Supplier is a Strategic Supplier, the Cabinet Office Markets and Suppliers Team;
“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;
"BCDR Plan"	

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

	<p>a plan which details the processes and arrangements that the Supplier shall follow to:</p> <ul style="list-style-type: none"> (a) ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and (b) the recovery of the Deliverables in the event of a Disaster;
"Business Continuity Plan"	has the meaning given to it in Paragraph 1.3.2 of Part B of this Schedule;
"Class 1 Transaction"	has the meaning set out in the listing rules issued by the UK Listing Authority;
"Control"	the possession by a 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;
"Corporate Change Event"	<p>means:</p> <ul style="list-style-type: none"> (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 Buyer, could have a material adverse effect on the Deliverables; (c) any change to the business of the Supplier or any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Deliverables; (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;

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

	<p>(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;</p> <p>(g) an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group;</p> <p>(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;</p> <p>(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</p> <p>(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;</p>
“Critical National Infrastructure”	<p>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:</p> <p>(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</p> <p>(b) significant impact on the national security, national defence, or the functioning of the UK;</p>

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

“Critical Service Contract”	a service contract which the Buyer has categorised as a Gold Contract using the Cabinet Office Contract Tiering Tool or which the Buyer otherwise considers should be classed as a Critical Service Contract;
“CRP Information”	means, together, the: Group Structure Information and Resolution Commentary; and UK Public Sector and CNI Contract Information;
“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 the Contract, including for the avoidance of doubt the provision of the Deliverables in accordance with the terms of the Contract;
"Disaster"	the occurrence of one or more events which, either separately or cumulatively, mean that the Deliverables, or a material part thereof will be unavailable (or could reasonably be anticipated to be unavailable);
"Disaster Recovery Deliverables"	the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Disaster Recovery Plan"	has the meaning given to it in Paragraph 1.3.3 of Part B of this Schedule;
"Disaster Recovery System"	the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
“Group Structure Information and Resolution Commentary”	means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 2 to 4 and Appendix 1 to Part C;

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

“Parent Undertaking”	has the meaning set out in section 1162 of the Companies Act 2006;
“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;
“Related Supplier”	any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;
“Review Report”	has the meaning given to it in Paragraph 6.3 of Part B of this Schedule;
“Standard BCDR Plan”	means the Supplier’s standard BCDR Plan;
“Strategic Supplier”	means those suppliers to government listed at https://www.gov.uk/government/publications/strategic-suppliers ;
“Subsidiary Undertaking”	has the meaning set out in section 1162 of the Companies Act 2006;
“Supplier Group”	means the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings;
“Supplier's Proposals”	has the meaning given to it in Paragraph 6.3 of Part B of this Schedule;
“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; and
“UK Public Sector / CNI Contract Information”	means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 2 to 4 of Part C and Appendix 2 of Part C;

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

Part A: BCDR Plan – Short Form

Unless otherwise specified in this Schedule, this Part A shall apply only to Call-Off Contracts which have been awarded via Direct Award in accordance with Framework Schedule 7 (Call-Off Contract Award Procedure).

1. BCDR Plan

- 1.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.
- 1.2 Promptly (and in any event within 30 days) after the Start Date, the Supplier shall provide to the Buyer its Standard BCDR Plan.
- 1.3 The Supplier shall ensure at all times that its Standard BCDR Plan conforms with Good Industry Practice.
- 1.4 The Supplier may from time to time during the Contract Period review, update, and/or test its Standard BCDR Plan. The Supplier shall ensure that any use by it or any Subcontractor of "live" Buyer Data in such testing is first approved with the Buyer. Copies of live test data used in any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.
- 1.5 The Supplier shall, within twenty (20) Working Days of the conclusion of each test of its Standard BCDR Plan, provide to the Buyer a report setting out:
 - 1.5.1 the outcome of the test;
 - 1.5.2 any failures in the Standard BCDR Plan (including the Standard BCDR Plan's procedures) revealed by the test; and
 - 1.5.3 the Supplier's proposals for remedying any such failures.
- 1.6 In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke its Standard BCDR Plan (and shall inform the Buyer promptly of such invocation). In all other instances the Supplier shall invoke or test the Standard BCDR Plan only with the prior consent of the Buyer.
- 1.7 To the extent the Standard BCDR Plan contains processes, procedures, and/or other content which is designed to permit the continuity of the business operations of the Buyer supported by the Deliverables through continued provision of the Deliverables following an Insolvency Event of the Supplier, any Key Sub-contractor and/or any Supplier, the Standard BCDR Plan shall be invoked by the Supplier:

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 Deliverables; and/or

where there is an Insolvency Event of the Supplier and the insolvency

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

arrangements enable the Supplier to invoke the plan.

PART A: ANNEX 1 Supplier BCDR Plan

By entering into the Contract the Buyer hereby confirms receipt of the BCDR Plan contained in the Contract in this Call-Off Schedule 8 (Business Continuity and Disaster Recovery) and acknowledges it as the Supplier's fulfillment of its obligations under paragraph 1.2 of this Schedule.



Vodafone UK

Business Resilience Whitepaper

Published: 19/10/2023
Version 5.0

Contents

1.	Executive Summary	2
2.	Major Incident Management	2
3.	Crisis Management	2
4.	Business Continuity Management	2
5.	Technology Resilience	3
6.	Information Security	4
7.	Cyber Security	4
8.	Physical & Personnel Security.....	4
9.	Risk Management	4



1. Executive Summary

Vodafone UK (VFUK) is committed to being a resilient organisation. We invest significant time and resource into ensuring that we are able to respond effectively to adverse events and recover quickly to enable us to continue to deliver business activities and critical services to our customers, whilst safeguarding our people, network and brand.

We view resilience as an overarching discipline that encompasses a number of interrelated activities and functions, including Business Continuity (BC) Management, Crisis Management, Technology Resilience and Physical and Personnel Security.

In order to ensure we measure ourselves against internationally recognised standards we invest in maintaining ISO certification across the areas that support our overarching resilience. We hold current ISO 22301, ISO 27001, ISO 9001, ISO 20000 certification.

2. Major Incident Management

VFUK experience Major Incidents (MI) across our fixed and mobile estate each year and we have an established process and team in place to deal with any such incident. An MI is an event that has significantly impacted, or has the potential to impact customers, either directly or indirectly.

The MI Team is staffed 24x7x365 to provide operational command and control of an MI to ensure it is dealt with in a timely manner, mitigating any impact that would be felt by our customers.

In the event that an MI escalates above and beyond pre-defined thresholds, a Crisis will be declared and will be supported by the Crisis Management (CM) Process.

3. Crisis Management

Vodafone UK have an established Crisis Management (CM) process as part of our Business Continuity Management System (BCMS). The process is flexible and can be activated to provide support in the event of any situation that poses a potential or actual threat to our business activities, services, customers, people, network or brand.

Within the CM Process we have a dedicated Crisis Team who co-ordinate and deliver CM, supported by nominated senior management personnel from across the business. All functions within the Crisis Team provide cover 24x7x365 and we regularly exercise and test our CM process to ensure we are ready to respond if and when needed.

VFUK have a dedicated Crisis Plan in place to support the CM process and this contains a number of pre-determined responses to specific crisis events that are continually improved based on experience and exercise learning.

4. Business Continuity Management

Vodafone UK has an established Business Continuity Management System (BCMS), certified to ISO 22301, that covers all our voice and data services. Through the delivery of a robust BCMS, we are able to deliver our business critical functions and services to pre-defined levels during disruptive incidents and crises.

The BCMS is delivered by a dedicated and experienced Team of BC professionals supported by functional co-ordinators to ensure the accurate capture of the elements that contribute to functional Business Impact Analysis (BIAs) and Business Continuity Plans (BCPs). VFUK ensure that every area within our corporate structure is included within functional BIAs and BCPs, all of which are subject to annual review and exercising.



We also subject our Supply Chain to stringent BCMS reviews to ensure supplier resilience. We expect our Suppliers to comply with the Vodafone Suppliers Business Continuity Policy, work to industry best practise for Business Continuity Management (ISO22301) and preferably be independently certified.

5. Technology Resilience

5.1 Our Network

Network Continuity

We use the latest technology to ensure our network is as resilient as possible with Network Operations Centres providing best in class network monitoring, management and service support. We work 24x7x365 to ensure that any issues on the network are identified, prioritised and addressed quickly and effectively so that any downtime is kept to a minimum.

Network Site Integrity

Our core network sites are equipped with physical and environmental control systems such as backup power systems, fire prevention and air conditioning to enable us to maintain the continuity of services that run through them.

Physical Controls

Our core sites are housed in secure premises which meet our physical security standards mandated by our dedicated Physical Security Team.

Environmental Controls

Our core sites have onsite generator backup capable of supporting the total electrical demand with an onsite fuel supply for multiple days as well as battery backup. The power design (generators, batteries and mains) and auto cutover are regularly tested to ensure uninterrupted power supply to all the core network equipment.

5.2 Mobile Network Resilience

The VFUK Mobile Network core is designed for reliability and availability, with design principles providing high availability operation at an element level within a site and geographic resilience at a network level ensuring platforms are not single points of failure. The network design is such that where a Radio Base Station provides a combination of 2G, 3G, 4G or 5G coverage, the site is connected to multiple Mobile Telephone Exchanges (MTX) to ensure continued availability even in the event of a complete MTX failure

5.3 Fixed Network Resilience

Our VFUK Fixed Network is a state-of-the-art converged network (known as RedStream) that provides connectivity for all our mobile, consumer and enterprise customers. The core network has been designed, built and tested with resilient equipment, physically diverse links and sites to offer high availability in the event of a failure, enabling us to maintain continuity of service to our customers.

To maximise the resilience benefits of our VFUK Fixed Network, customers should carefully consider their desired level of service availability and resilience when purchasing services from VFUK, such as dual access or backup links from the customer premise(s) to our network sites which will be more resilient than single access links. Further information on resilience options is available from your Account Management Team.

5.4 Our IT Systems

The VFUK IT Operations function is aligned to ITIL Service Management processes such as Risk, Change, Incident and Problem management with escalation and notification processes in place to assess and oversee the co-ordination of the response to any potential risk or service impacting events that may occur.

The categorisation of our VFUK IT systems is based on the criticality of the business processes that they support, with internal service level agreements and key performance indicators defined.



A framework for testing the technical capability of our systems is in place. A key objective of the framework is to maintain team and technical levels of preparedness in order to respond to incidents, which have the potential to impact service to our customers.

6. Information Security

VFUK run an Information Security Management System (ISMS) in line with the recommendations and requirements of ISO 27001. Our ISMS ensures that we have a systematic approach to managing confidential and sensitive information to ensure it remains secure at all times.

7. Cyber Security

VFUK Cyber Security's mission is to protect Vodafone People, Technology and Process. Through dedicated teams of Governance, Architecture, Consultancy and Operations it delivers the life cycle of; Plan, Design, Build, Run and Check, to deliver our technical solution (security by design) and support VFUK in fulfilling its legal and regulatory requirements.

Included in the Cyber Security function is a Security Operations Centre (SOC), supported by a dedicated intelligence function that combines internal expertise with best-in-class vendor support in order to ensure we protect our network and associated functions. The SOC and intelligence teams liaise closely with their opposite numbers in Vodafone Group, allowing us to expand our coverage of global threats that could pose a risk to VFUK technology.

8. Physical & Personnel Security

VFUK have a dedicated Physical Security Team in place who are responsible for ensuring that our estate meets our physical security standards to ensure that we adequately protect our people and network. Their responsibilities include annual audits of our critical estate, the monitoring of access control and the setting of our minimum physical security standard baselines through a suite of Policies, Standards and Procedures. To further enhance our physical security infrastructure, we have a dedicated 24x7x365 Security Operations Centre (V-SOC) to provide live monitoring and management of our sites and their access, as well as provide situational updates to our field-based teams and assist in the coordination of any blue light responses.

We take our security culture seriously and continually manage internal security roadshows which is further supported by regular awareness campaigns to ensure our people act within our security culture and principals. In addition, all employees complete Annual Security training as part of Vodafone UK's 'Doing What's Right' training

9. Risk Management

VFUK operates a 'Three Lines of Defence' governance model for the management and oversight of risk. A robust risk management framework is in place to ensure risks are identified and mitigated or controlled appropriately. Risks are recorded on business area risk registers and managed through the workflow of our risk management system. This ensures a consistent methodology for measuring risk is applied and provides valuable risk reporting capabilities. Specialist risk management resources are deployed throughout the business including within centralised risk teams in 1st and 2nd Lines and dedicated business support through defined Risk Champion roles.

End of document



Current issue date:
Expiry date:
Certificate identity number:

19 October 2023
18 October 2026
10541828

Original approval(s):
ISO 22301 - 24 February 2014

Certificate of Approval

This is to certify that the Management System of:

Vodafone Ltd

Vodafone House, The Connection, Newbury, RG14 2FN, United Kingdom

has been approved by LRQA to the following standards:

ISO 22301:2019

Approval number(s): ISO 22301 – 0008735

This certificate is valid only in association with the certificate schedule bearing the same number on which the locations applicable to this approval are listed.

The scope of this approval is applicable to:

Voice and data services provided by Vodafone UK for its global telecommunications services.

Marta Escudero

Regional Director, United Kingdom and Americas (UKAM)

Issued by: LRQA Limited





Certificate identity number: 10541828

Certificate Schedule

Location	Activities
Office: Newbury, HQ Vodafone House, The Connection, Newbury, RG14 2FN, United Kingdom	ISO 22301:2019 Voice and data services provided by Vodafone UK for its global telecommunications services.
Office: Bracknell, Waterside House Waterside House, Waterside Park, Longshot Lane, Bracknell, RG12 1XL, United Kingdom	ISO 22301:2019 Voice and data services provided by Vodafone UK for its global telecommunications services.
Office: Leeds Melbourne Street, Leeds, LS2 7PS, United Kingdom	ISO 22301:2019 Voice and data services provided by Vodafone UK for its global telecommunications services.
Office: London The Speechmark The Speechmark, 114 Great Suffolk Street, London, SE1 0SL, United Kingdom	ISO 22301:2019 Voice and data services provided by Vodafone UK for its global telecommunications services.
Retail Operations The Connection, Newbury, RG14 2FN, United Kingdom	ISO 22301:2019 Voice and data services provided by Vodafone UK for its global telecommunications services.
Office: Stoke Shelton Boulevard, Festival Park, Stoke-on-Trent, ST1 5PZ, United Kingdom	ISO 22301:2019 Voice and data services provided by Vodafone UK for its global telecommunications services.
Data Centre: Swindon SDN ISC Galileo Centre, The Computer Centre, Windmill Hill Business Park, Swindon, SN5 6LA, United Kingdom	ISO 22301:2019 Voice and data services provided by Vodafone UK for its global telecommunications services.
Warrington Workshop Unit 2, Kingsland Grange, Warrington, WA1 4RW, United Kingdom	ISO 22301:2019 Voice and data services provided by Vodafone UK for its global telecommunications services.



0001



Certificate identity number: 10541828

Certificate Schedule

Location	Activities
Beacon Hill Office Park, Cafferata Way, Newark, Nottinghamshire, NG24 2TN, United Kingdom	ISO 22301:2019 Voice and data services provided by Vodafone UK for its global telecommunications services.
Manchester Business Park, Aviator Way, 3000 Aviator Way, Wythenshawe, Manchester, M22 5TG, United Kingdom	ISO 22301:2019 Voice and data services provided by Vodafone UK for its global telecommunications services.
300 Bath Street, Glasgow, G2 4JR, United Kingdom	ISO 22301:2019 Voice and data services provided by Vodafone UK for its global telecommunications services.
Office: Birmingham Small Heath Unit 1, Small Heath Business Park, Talbot Way, Small Heath, Birmingham, B10 0HJ, United Kingdom	ISO 22301:2019 Voice and data services provided by Vodafone UK for its global telecommunications services.



Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

Part B: BCDR Plan - Long Form

Not applicable.

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

Part C: Corporate Resolution Planning

This Part C shall apply to all Call-Off Contracts.

1. Service Status and Supplier Status

- 1.1 This Contract 'is not' a Critical Service Contract.
- 1.2 The Supplier shall notify the Buyer in writing within 5 Working Days of the Effective Date and throughout the Call-Off Contract Period 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

- 2.1 Paragraphs 2 to 4 of this Part C shall apply if the Contract has been specified as a Critical Service Contract under Paragraph 1.1 of this Part C 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 C:
 - 2.2.1 where the Contract is a Critical Service Contract, the Supplier shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the Effective Date; and
 - 2.2.2 except where it has already been provided, where the Supplier is a Public Sector Dependent Supplier, it shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the date of the Appropriate Authority's or Appropriate 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:
 - 2.3.1 is full, comprehensive, accurate and up to date;
 - 2.3.2 is split into two parts:
 - (a) Group Structure Information and Resolution Commentary;
 - (b) UK Public Service / CNI Contract Information and is structured and presented in accordance with the requirements and explanatory notes set out at Annex I of the latest published version of the Resolution Planning Guidance published by the Cabinet Office Government Commercial Function and available at <https://www.gov.uk/government/publications/the-outsourcingplaybook> and contains the level of detail required (adapted as necessary to the Supplier's circumstances);
 - 2.3.3 incorporates any additional commentary, supporting documents and evidence which would reasonably be required by the Appropriate

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

- Authority or Appropriate Authorities to understand and consider the information for approval;
- 2.3.4 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 Critical National Infrastructure and the nature of those agreements; and
 - 2.3.5 complies with the requirements set out at Appendix 1 (Group Structure Information and Resolution Commentary) and Appendix 2 (UK Public Sector / CNI Contract Information) respectively.
- 2.4 Following receipt by the Appropriate Authority or Appropriate Authorities of the CRP Information pursuant to Paragraphs 2.2, 2.8 and 2.9 of this Part C, the Buyer shall procure that the Appropriate Authority or Appropriate Authorities shall 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 the Appropriate Authority or Appropriate Authorities approves the CRP Information or that the Appropriate Authority or Appropriate Authorities rejects the CRP Information.
- 2.5 If the Appropriate Authority or Appropriate Authorities rejects the CRP Information:
- 2.5.1 the Buyer 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
 - 2.5.2 the Supplier shall revise the CRP Information, taking reasonable account of the Appropriate Authority's or Appropriate Authorities' comments, and shall re-submit the CRP Information to the Appropriate Authority or Appropriate Authorities for approval within 30 days of the date of the Appropriate Authority's or Appropriate Authorities' rejection. The provisions of paragraph 2.3 to 2.5 of this Part C shall apply again to any resubmitted CRP Information provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure under Clause 34 of the Core Terms 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 (which has the meaning in paragraph 2.7 below) 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 of this Part C if it provides a copy of the Valid Assurance to the Appropriate Authority or Appropriate Authorities on or before the date on which the CRP Information would otherwise have been required.

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

- 2.7 An Assurance shall be deemed Valid for the purposes of Paragraph 2.6 of this Part C if:
 - 2.7.1 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
 - 2.7.2 no Corporate Change Events or Financial Distress Events (or events which would be deemed to be Corporate Change Events or Financial Distress Events if the Contract had then been in force) have occurred since the date of issue of the Assurance.
- 2.8 If the Contract is a Critical Service Contract, the Supplier shall provide an updated version of the CRP Information (or, in the case of Paragraph 2.8.3 of this Part C its initial CRP Information) to the Appropriate Authority or Appropriate Authorities:
 - 2.8.1 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 C) unless the Supplier is relieved of the consequences of the Financial Distress Event under Paragraph 7.1 of Joint Schedule 7 (Financial Distress) (if applicable);
 - 2.8.2 within 30 days of a Corporate Change Event unless not required pursuant to Paragraph 2.10 of this Part C;
 - 2.8.3 within 30 days of the date that:
 - (a) 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 of this Part C; or
 - (b) none of the credit rating agencies specified at Paragraph 2.10 of this Part C hold a public credit rating for the Supplier or any of its Parent Undertakings; and
 - 2.8.4 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 Appropriate Authority (whichever is the earlier), unless:
 - (a) updated CRP Information has been provided under any of Paragraphs 2.8.1 2.8.2 or 2.8.3 of this Part 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 2.8.4 of Part C; or
 - (b) unless not required pursuant to Paragraph 2.10 of this Part C.
- 2.9 Where the Supplier is a Public Sector Dependent Supplier and the Contract is not a Critical Service Contract, then on the occurrence of any of the events specified in Paragraphs 2.8.1 to 2.8.4 of this Part C, the Supplier shall provide

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

at the request of the Appropriate Authority or Appropriate 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 Buyer), the CRP Information to the Appropriate Authority or Appropriate Authorities.

- 2.10 Where the Supplier or a Parent Undertaking of the Supplier has a credit rating of either:

2.10.1 Aa3 or better from Moody's;

2.10.2 AA- or better from Standard and Poors;

2.10.3 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 Annex 3 to Joint Schedule 7 (Financial Distress), if applicable) or (ii) the Supplier and its Parent Undertakings cease to fulfil the criteria set out in this Paragraph 2.10 of this Part C, in which cases the Supplier shall provide the updated version of the CRP Information in accordance with paragraph 2.8 of this Part C.

- 2.11 Subject to Paragraph 4 of this Part C, where the Supplier demonstrates to the reasonable satisfaction of the Appropriate Authority or Appropriate Authorities that a particular item of CRP Information is highly confidential, the Supplier may, having orally disclosed and discussed that information with the Appropriate Authority or Appropriate Authorities, redact or omit that information from the CRP Information provided that if a Financial Distress Event occurs, this exemption shall no longer apply and the Supplier shall promptly provide the relevant information to the Appropriate Authority or Appropriate Authorities to the extent required under Paragraph 2.8 of this Part C.

3. Termination Rights

- 3.1 The Buyer shall be entitled to terminate the Contract if the Supplier is required to provide CRP Information under Paragraph 2 of this Part C and either:

3.1.1 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 Appropriate Authority's or Appropriate Authorities' request; or

3.1.2 the Supplier fails to obtain an Assurance from the Appropriate Authority or Appropriate Authorities within 4 months of the date that it was first required to provide the CRP Information under the Contract,

which shall be deemed to be an event to which Clause 10.4.1 of the Core Terms applies and Clauses 10.6.1 and 10.6.2 of the Core Terms shall apply accordingly.

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

4. Confidentiality and usage of CRP Information

- 4.1 The Buyer 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 Appropriate Authority is the Cabinet Office Markets and Suppliers Team, at the Supplier's request, the Buyer 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 Buyer under paragraph 4.1 of this Part C and Clause 15 of the Core Terms.
- 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 Appropriate Authority or Appropriate Authorities pursuant to Paragraph 2 of this Part C subject, where necessary, to the Appropriate Authority or Appropriate 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 C, 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:
 - 4.4.1 redacting only those parts of the information which are subject to such obligations of confidentiality;
 - 4.4.2 providing the information in a form that does not breach its obligations of confidentiality including (where possible) by:
 - (a) summarising the information;
 - (b) grouping the information;
 - (c) anonymising the information; and
 - (d) presenting the information in general terms
- 4.5 The Supplier shall provide the Appropriate Authority or Appropriate 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.

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

Appendix 1: Group structure information and resolution commentary

1. The Supplier shall:

- 1.1 provide sufficient information to allow the Appropriate Authority to understand the implications on the Supplier Group's UK Public Sector Business and CNI contracts listed pursuant to Appendix 2 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 Appendix 2 and the dependencies between each.

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Call-Off Ref:

Crown Copyright 2021

Appendix 2: UK Public Sector / CNI Contract Information

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:
 - 1.1.1 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;
 - 1.1.2 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 1.1.1 of this Appendix 2 and where the member of the Supplier Group is acting as a key sub-contractor under the agreement with the end recipient; or
 - 1.1.3 involve or could reasonably be considered to involve CNI;
 - 1.2 provide the Appropriate 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.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

Call-Off Schedule 9 (Security)

Part A: Short Form Security Requirements

1. Definitions

- 1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Breach of Security"	<p>the occurrence of:</p> <ul style="list-style-type: none"> a) any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, <p>in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2;</p>
"Security Management Plan"	<p>the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time.</p>

2. Complying with security requirements and updates to them

- 2.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

Framework Ref: RM6116

Project Version:

Model Version: v3.4

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

- 2.2 The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.
- 2.3 Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.
- 2.4 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. 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 be subject to the Variation Procedure.
- 2.5 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

3. Security Standards

- 3.1 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.
- 3.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:
 - 3.2.1 is in accordance with the Law and this Contract;
 - 3.2.2 as a minimum demonstrates Good Industry Practice;
 - 3.2.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and
 - 3.2.4 where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.
- 3.3 The references to standards, guidance and policies contained or set out in Paragraph 3.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.
- 3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

4. Security Management Plan

4.1 Introduction

- 4.1.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

4.2 Content of the Security Management Plan

4.2.1 The Security Management Plan shall:

- a) comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;
- b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;
- c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
- d) be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer 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 Deliverables;
- e) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;
- f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and
- g) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

4.3 Development of the Security Management Plan

- 4.3.1 Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.
- 4.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.
- 4.3.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 4.3.2. However a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.
- 4.3.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3.2 or of any change to the Security Management Plan in accordance with Paragraph 4.4 shall not relieve the Supplier of its obligations under this Schedule.

4.4 Amendment of the Security Management Plan

- 4.4.1 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:
- a) emerging changes in Good Industry Practice;
 - b) any change or proposed change to the Deliverables and/or associated processes;
 - c) where necessary in accordance with paragraph 2.2, any change to the Security Policy;
 - d) any new perceived or changed security threats; and
 - e) any reasonable change in requirements requested by the Buyer.
- 4.4.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

- a) suggested improvements to the effectiveness of the Security Management Plan;
- b) updates to the risk assessments; and
- c) suggested improvements in measuring the effectiveness of controls.

4.4.3 Subject to Paragraph 4.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

4.4.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

5. Security breach

5.1 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

5.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:

- 5.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:
 - a) minimise the extent of actual or potential harm caused by any Breach of Security;
 - b) remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;
 - c) prevent an equivalent breach in the future exploiting the same cause failure; and
 - d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

attempted Breach of Security, including a cause analysis where required by the Buyer.

- 5.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with paragraph 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

Vodafone Network Services 3 Framework (RM6116) Security Management Plan

Introduction:

We have come a long way since making the first ever mobile call in the UK on 1 January 1985. Today, Vodafone has more than 500 million customers around the world. In 30 years, a small mobile operator in Newbury has grown into a global business operating in 26 countries and partner with networks in over 45 more.

In an increasingly connected world, it is no longer just about a domestic customer being able to talk and text. Our global network allows Customers to share images and videos securely around the World as soon as they're captured. And because we now do more than just mobile, more customers look to Vodafone for great value in their fixed and converged solutions. Some of our larger Enterprise Customers operate in multiple countries so we need to ensure these services are delivered securely.

Detailed below is information of how Vodafone's meets the requirements of Call-Off Schedule 9 (Security), detailing specifically the relevant clauses of Call-Off Schedule 9 and how Vodafone meets the requirements.

Security Posture:

Vodafone are committed to providing world-class security. We deliver some of the most secure telecommunications services in the world and have a proven record for delivering trusted mission-critical services to a wide range of customers, including government, utility, finance, and retail sectors. Our dedicated Security teams in both Group and UK work tirelessly together to ensure our customers are protected from security threats and can continue to operate in an event of a disaster.

Vodafone operates an Information Security Management System (ISMS) based on and, certified complaint with ISO27001:2013, including risk management, business continuity, incident management, physical security, security awareness training and much more. This document supports Mobile Voice and Data Services Frameworks (RM6261) setting out how Vodafone manages security against Call of Schedule 9 Security clauses, this should be referenced alongside our ISO27001:2013 certificate and accompanying Statement of Applicability (SoA).

How we Manage Security in accordance with Schedule 9:

1. Complying with security requirements and updates to them

- 1.1 The Supplier shall comply with the Security Policy and the requirements in this Schedule including the Security Management Plan and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

Vodafone offer secure services that are independently audited by external accreditation bodies against ISO27001:2013

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

- 1.2 The Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

Vodafone welcome every opportunity to work with our customers and ensure the security and quality of our service exceed customer expectations.

- 1.3 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. 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 be subject to the Variation Procedure.

Vodafone welcome every opportunity to work with our customers and ensure the security and quality of our service exceed customer expectations.

- 1.4 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

Vodafone welcome every opportunity to work with our customers and ensure the security and quality of our service exceed customer expectations.

2. Security Standards

- 2.1 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.

Vodafone is committed to providing world class services. We go to great lengths to ensure our products and services meet the highest levels of confidentiality, integrity and availability and demonstrate this through successfully gaining and maintain ISO27001:2013 certification.

- 2.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

2.2.1. is in accordance with the Law and this Contract;

Vodafone fully complies with all legislation and regulations for all local markets in which we operate.

2.2.2. as a minimum demonstrates Good Industry Practice;

Vodafone successfully gained and maintains certification against ISO9001, ISO20000, ISO22301, ISO27001

2.2.3. meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and

Vodafone successfully gained and maintains certification against Cyber Essentials Plus complies with the Security Policy and the ICT Policy.

Vodafone are confident we met the requirements of the Security Policy and ICT Policy as evidenced by our commitment to maintaining ISO27001:2013

2.2.4. The references to standards, guidance and policies contained or set out in

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

Paragraph 3.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

Vodafone is committed to maintaining legislative and regulatory compliance, and continuing to maintain our certifications and adherence to good practice

2.2.5. In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

Vodafone continually monitor our network and services and will take immediate action to address any incidents that may impact those services. In the event an incident has an impact upon a customer(s), our Incident Management processes will trigger notification of affected customers.

3. Security Management Plan

3.1 Introduction

3.1.1. The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

Vodafone management of our ISMS and security policies is overseen by the Security Management Review, which meets monthly, and includes senior representatives from across the company.

3.2 Content of the Security Management Plan

3.2.1. The Security Management Plan shall:

- a) comply with the principles of security set out in Paragraph 3. and any other provisions of this Contract relevant to security;

Vodafone are committed to maintaining our ISO27001:2013.

- b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;

Vodafone are committed to providing world-class security. We deliver some of the most secure telecommunications services in the world and have a proven record for delivering trusted mission-critical services to a wide range of customers, including government, utility, finance, and retail sectors. Our dedicated Security teams in both Group and UK work tirelessly together to ensure our customers are protected from security threats and can continue to operate in an event of a disaster.

Vodafone Group Corporate Security set over arching information security policy and directly support Vodafone Group Business Customers.

Vodafone Global Cyber Security implement and monitor technical security controls and respond to security incidents at a Global / Group level.

Vodafone Corporate Security UK set information security policy for the UK, manage information security and business continuity, external certifications, fraud, disclosures and security investigations.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

Vodafone Cyber Security UK implement and monitor technical security controls and respond to security incidents for the UK

- c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

Vodafone requires our suppliers to sign up to comply with Vodafone policies including Information Security, Business Continuity, and Code of Ethics.

- d) be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer 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 Deliverables;

Vodafone is a Global company and has a Global Information Security policy owned jointly by the Global Cyber Security Director & Group Corporate Security Director, approved by the Group Chief Technology Officer. This sets out the minimum requirements for Vodafone Group and Local Markets to comply with.

The UK Information Security policy builds upon the Vodafone Group policy and overlays UK Legislation and Regulation obligations is owned by the Head of Cyber Security UK and is approved by Chief Technology Officer.

- e) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;

Vodafone management of our ISMS and security policies is overseen by the Security Management Review, which meets monthly, and includes senior representatives from across the company.

Compliance and performance against our ISMS is monitored and tested by our security teams:

Corporate Security, manage security and business continuity certificates across the company.

Cyber Security, manage technology security risks and implementation of security controls across the company.

Framework Ref: RM6116

Project Version:

Model Version: v3.4

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

- f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and the Security Policy; and

Vodafone management of our ISMS and security policies is overseen by the Security Management Review, which meets monthly, and includes senior representatives from across the company.

Changes to policy and security plans will be governed under Change Control via the Security Management Review.

- g) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

3.3 Development of the Security Management Plan

- 3.3.1. Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.

Vodafone has held ISO27001 certification since 2005 and our Information Security Management System has been assessed by independent accreditation bodies annually.

3.4 Amendment of the Security Management Plan

- 3.4.1. The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:

- a) emerging changes in Good Industry Practice;
- b) any change or proposed change to the Deliverables and/or associated processes;
- c) any change to the Security Policy;
- d) any new perceived or changed security threats; and
- e) any reasonable change in requirements requested by the Buyer.

Vodafone policies are reviewed at least annually or on significant change within Vodafone or the landscape we operate in to ensure they are accurate, up to date and effective.

- 3.4.2. The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

- a) suggested improvements to the effectiveness of the Security Management Plan;
- b) updates to the risk assessments; and

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

c) suggested improvements in measuring the effectiveness of controls.

Vodafone are committed to maintaining our ISO27001:2013 . Our independent accreditation partners audit our compliance annually and we publish our certificates on our website.

3.4.3. Subject to Paragraph 4.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure. Vodafone management of our ISMS and security policies is overseen by the Security Governance Board, which meets bi-monthly, and includes senior representatives from across the company.

Changes to policy and security plans will be governed under Change Control via the Security Management Review.

3.4.4. The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

4. Security breach

4.1 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

Vodafone will agree lines of communications for incidents and security incidents. Vodafone Network Management and Incident Management teams are available and can be contacted 24x7

4.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:

4.2.1. immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

a) minimise the extent of actual or potential harm caused by any Breach of Security;

Defined processes exist to prioritise incidents based on the impact to Vodafone customers and business. Security teams have visibility of incidents and may declare an incident a security incident and escalate the priority accordingly.

b) remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;

Defined processes exist to prioritise incidents based on the impact to Vodafone customers and business. Security teams have visibility of incidents and may declare an incident a security incident and escalate the priority accordingly.

Call-Off Schedule 9 (Security)

Call-Off Ref:

Crown Copyright 2018

- c) prevent an equivalent breach in the future exploiting the same cause failure; and

Vodafone perform post incident reviews on all incidents prioritised as medium or above to learn lessons and implement mitigations to prevent further occurrence of the incident.

- d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

Vodafone will agree lines of communications for incidents and security incidents. Vodafone Network Management and Incident Management teams are available and can be contacted 24x7

- 4.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security policy or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

Part B: Long Form Security Requirements

Not used.

Call-Off Schedule 9 (Security)
Call-Off Ref:
Crown Copyright 2018

Call-Off Schedule 11 (Installation Works)
Call-Off Ref:
Crown Copyright 2018

Call-Off Schedule 11 (Installation Works)

1. When this Schedule should be used

- 1.1. This Schedule is designed to provide additional provisions necessary to facilitate the provision of Deliverables requiring installation by the Supplier.

2. How things must be installed

- 2.1. Where the Supplier reasonably believes, it has completed the Installation Works it shall notify the Buyer in writing. Following receipt of such notice, the Buyer shall inspect the Installation Works and shall, by giving written notice to the Supplier:
 - 2.1.1. accept the Installation Works, or
 - 2.1.2. reject the Installation Works and provide reasons to the Supplier if, in the Buyer's reasonable opinion, the Installation Works do not meet the requirements set out in the Call-Off Order Form (or elsewhere in this Contract).
- 2.2. If the Buyer rejects the Installation Works in accordance with Paragraph 2.1.2, the Supplier shall immediately rectify or remedy any defects and if, in the Buyer's reasonable opinion, the Installation Works do not, within five (5) Working Days of such rectification or remedy, meet the requirements set out in the Call-Off Order Form (or elsewhere in this Contract), the Buyer may terminate this Contract for material Default.
- 2.3. The Installation Works shall be deemed to be completed when the Supplier receives a notice issued by the Buyer in accordance with Paragraph 2.1.1 Notwithstanding the acceptance of any Installation Works in accordance with Paragraph 2.1.1), the Supplier shall remain solely responsible for ensuring that the Goods and the Installation Works conform to the specification in the Call-Off Order Form (or elsewhere in this Contract). No rights of estoppel or waiver shall arise as a result of the acceptance by the Buyer of the Installation Works.
- 2.4. Throughout the Contract Period, the Supplier shall have at all times all licences, approvals and consents necessary to enable the Supplier and the Supplier Staff to carry out the Installation Works.

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

Call-Off Schedule 14 (Service Levels)**1. Introduction**

1.1 The Buyer will specify in the Order Form at Further Competition whether Part A or Part B to this Schedule applies or may opt to adopt the Supplier's offer or Core Terms by omitting this Schedule.

2. Definitions

2.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

“Achieved Service Level”	means the actual level of performance of a Service achieved by the Supplier in relation to a Service Level Performance Criteria for a Service Period;
“Agreed Service Time”	means the period during which the Supplier ensures the Services are Available to the Buyer;
“Available”	a Service shall be “Available” when the Buyer's end users are able to access and use all its functions at a level that enables them to carry out their normal duties. Availability shall be construed accordingly;
“Call-Off Contract Year”	means a consecutive period of twelve (12) Months commencing on the Call-Off Start Date or each anniversary thereof;
“Critical Service Level Failure”	a) Specified by the Buyer where the Buyer selects Part A to this Call-Off Schedule 14; or b) any instance of critical service level failure specified in Annex 2 to Part B of this Schedule where the Buyer selects Part B to this Schedule;

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

"Downtime"	means any period of time within the Agreed Service Time during which a Service is not Available, excluding Planned Downtime
"Imposed Carrier Downtime"	means time during which the Supplier is prevented from supplying the Services due to unavailability of an underlying telecommunications service from a third-party provider on which the Services are dependent. In any instance where the Supplier claims Imposed Carrier Downtime, the Supplier must be able to provide evidence to the satisfaction of the Buyer that the interruption to the Services was in fact due in its entirety to unavailability of the underlying service;
"Incident"	means an unplanned incident or interruption to Services, reduction in the quality of the Services or event which could affect the Services in the future;
"Incident Resolution Time"	means the time taken by the Supplier to Resolve an Incident, as set out in this Schedule;
"Planned Downtime"	means the time agreed in advance in writing by the Supplier and Buyer within the Agreed Service Time when a Service is not Available;
"Provisioning"	means the time taken from the placement of an Order for a Service or part thereof until the Service is Available to the Buyer and Provision shall be construed accordingly;
"Resolution"	means an action taken by or on behalf of the Supplier to fully repair the root cause of an Incident or to implement a workaround, such that the Services are returned to being Available. Resolve and Resolved shall be construed accordingly;
"Service Credits"	a) any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels; or

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

	b) any service credits specified in the Annex to Part B of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels;
"Service Credit Cap"	<p>a) in the period from the Call-Off Start Date to the end of the first Call-Off Contract Year fifteen thousand pounds (£15,000); and</p> <p>b) during the remainder of the Call-Off Contract Period, thirty five percent (35%) of the Charges payable to the Supplier under this Call-Off Contract in the period of twelve (12) Months immediately preceding the Service Period in respect of which Service Credits are accrued;</p> <p>unless otherwise stated in the Order Form during a Further Competition;</p>
"Service Desk"	means the single point of contact set up and operated by the Supplier to log, monitor and escalate Incidents and Incident Resolutions;
"Service Failure Threshold"	means the level of performance of a Service which becomes unacceptable to the Buyer, including as set out in each Service Level Performance Criteria and where the Supplier fails to provide the Services in accordance with this Contract;
"Service Levels"	means any service levels applicable to the provision of the Services under this Call-Off Contract specified in Call-Off Schedule 14 (Service Levels);
"Service Level Failure"	means a failure to meet the Service Level Threshold in respect of a Service Level Performance Criterion;
"Service Level Threshold"	shall be as set out against the relevant Service Level in Annex 1 to Part A of this Schedule, or Annex 1 of Part B of this Schedule depending upon which option is selected by the Buyer;

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

“Service Period”	means a recurrent period of one month during the Call-Off Contract Period, unless otherwise specified in the Order Form;
“Unavailable”	in relation to a Service, means that the Service is not Available;

3. What happens if you don't meet the Service Levels

- 3.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Threshold for each Service Level.
- 3.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A or Part B of this Schedule, as appropriate, including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to meet any Service Level Threshold.
- 3.3 The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part C (Performance Monitoring) of this Schedule.
- 3.4 A Service Credit shall be the Buyer's exclusive financial remedy for a Service Level Failure except where:
 - 3.4.1 the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or
 - 3.4.2 the Service Level Failure:
 - (a) exceeds the relevant Service Failure Threshold;
 - (b) has arisen due to a Prohibited Act or wilful Default by the Supplier;
 - (c) results in the corruption or loss of any Government Data; and/or
 - (d) results in the Buyer being required to make a compensation payment to one or more third parties; and/or
 - 3.4.3 the Buyer is entitled to or does terminate this Contract pursuant to Clause 10.4 of the Core Terms (CCS and Buyer Termination Rights).
- 3.5 Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months' notice, change the weighting of Service Level Threshold in respect of one or more Service Levels and

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:

- 3.5.1 the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;
- 3.5.2 the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards; and
- 3.5.3 there is no change to the Service Credit Cap.

4. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

- 4.1 any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and
- 4.2 the Buyer shall (subject to the Service Credit Cap) be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period ("**Compensation for Critical Service Level Failure**"), provided that the operation of this paragraph 4 shall be without prejudice to the right of the Buyer to terminate this Contract and/or to claim damages from the Supplier for material Default.

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

Part A: Short Form Service Levels and Service Credits

Not applicable.

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

PART B: Long Form Service Levels and Service Credits

1. General provisions

1.1. The Supplier shall provide support and advice, when required by the Buyer, on matters relating to:

- 1.1.1. Availability of the Services;
- 1.1.2. quality of the Services;
- 1.1.3. provisioning;
- 1.1.4. essential downtime
- 1.1.5. Buyer support;
- 1.1.6. complaints handling; and
- 1.1.7. accurate and timely invoices.

1.2. The Supplier accepts and acknowledges that failure to meet the Service Level Threshold set out in this Part B of this Call-Off Schedule will result in Service Credits being due to the Buyer.

2. Principal points

2.1. The objectives of the Service Levels and Service Credits are to:

- 2.1.1. incentivise the Supplier to meet the Service Levels and to remedy any failure to meet the Service Levels expeditiously;
- 2.1.2. ensure that the Services are of a consistently high quality and meet the requirements of the Buyer;
- 2.1.3. provide a mechanism whereby the Buyer can attain meaningful recognition of inconvenience and/or loss resulting from the Supplier's failure to deliver the level of service for which it has contracted to deliver; and
- 2.1.4. provide an incentive to the Supplier to comply with and to expeditiously remedy any failure to comply with the Service Levels.

2.2. The Parties acknowledge that:

- 2.2.1. The Buyer will, in all cases, prefer to receive the Services within the Service Levels in preference to receiving the Service Credits; and

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

2.2.2. the Supplier shall, in all cases, seek to deliver the Services within the Service Levels in preference to accepting a liability for Service Credits.

3. Service Levels

3.1. The Supplier shall monitor its performance under this Call-Off Contract by reference to the relevant Service Level Performance Criteria for achieving the Service Levels and shall send the Buyer a Performance Monitoring Report detailing the level of service which was achieved in accordance with the provisions of Part C (Performance Monitoring) of this Call-Off Schedule.

3.2. The Supplier shall, at all times, provide the Services in such a manner that the Service Level Thresholds are achieved.

3.3. If the level of performance of the Supplier of any element of the provision by it of the Services during the Call-Off Contract period:

3.3.1. is likely to or fails to meet any Service Level Threshold; or

3.3.2. is likely to cause or causes a Critical Service Level Failure to occur, the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without prejudice to any other of its rights howsoever arising may:

- a) Require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring; and
- b) If the action taken under paragraph require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring; and above has not already prevented or remedied the Service Level Failure or Critical Service Level Failure, the Buyer shall be entitled to instruct the Supplier to comply with the Rectification Plan Process; or
- c) If a Service Level Failure has occurred, deduct from the Call-Off Contract Charges the applicable Service Credits payable by the Supplier to the Buyer in accordance with the calculation formula set out in Annex 1 of this Part B of this Call-Off Schedule; or

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

- d) If a Critical Service Level Failure has occurred, exercise its right to compensation for such non-availability of Services via this Call-Off Contract.

3.4. Approval and implementation by the Buyer of any Rectification Plan shall not relieve the Supplier of any continuing responsibility to achieve the Service Levels, or remedy any failure to do so, and no estoppels or waiver shall arise from any such Approval and/or implementation by the Buyer.

3.5. The Buyer may enhance or otherwise modify the Service Levels required during a Further Competition Procedure.

3.6. The Services are subject to the following four Service Level Performance Criteria as set out in paragraph 6 of this Part B of Call-Off Schedule 14:

3.6.1. Availability;

3.6.2. Incident Resolution;

3.6.3. Quality; and

3.6.4. Provisioning.

4. Agreed Service Time

4.1. The Services will be made Available by the Supplier to the Buyer during the Agreed Service Time.

4.2. The Agreed Service Time applied to the Services will be determined by the Service Maintenance Level selected by the Buyer on the Order Form.

4.3. The Service Maintenance Levels and associated Agreed Service Times is set out in the following table:

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

Service Maintenance Level	Agreed Service Time
Level 1	Monday – Friday (excluding Bank Holidays) 08:00-18:00
Level 2	Monday – Saturday (excluding Bank Holidays) 08:00-18:00
Level 3	Monday – Sunday (including Bank Holidays) 07:00-21:00
Level 4	Monday – Sunday (including Bank Holidays); 00:00-23:59 (24 hours per day, 7 days per week)

5. Incidents

5.1. If the Services become Unavailable, the Buyer must report the Unavailability as an Incident to the Service Desk.

5.2. Incidents must be classified to one of the following four severity levels:

Severity Level	Description of impact of Incident
Severity 1	The Services are Unavailable across the entire Buyer's estate
Severity 2	The Services are Unavailable at one of the Buyer's sites
Severity 3	The Services are Unavailable to an individual user

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:
Crown Copyright 2018

Severity 4	All other Incidents, including any Incidents raised initially at a higher Severity Level that were subsequently deemed to be attributable to the Buyer or in any other way not attributable to the Supplier.
------------	--

5.2.1. The Supplier shall manage the Incident to resolution in accordance with this Call-Off Schedule, whilst keeping the Buyer appropriately informed of progress.

6. Service Level Performance Criteria

6.1. Availability

6.1.1. The Supplier shall ensure that the Services are Available during the Agreed Service Time.

6.1.2. Achieved Availability is calculated as a percentage of the total time in a Service Period that the Services should have otherwise been Available to the Buyer using the following formula:

$$\text{Achieved Availability \%} = \frac{(\text{MP} - \text{SD}) \times 100}{\text{MP}}$$

Where:

MP means total time within the Agreed Service Time (excluding Planned Downtime, Imposed Carrier Downtime and any Unavailability attributable to Severity 3 or Severity 4 Incidents) within the relevant Service Period; and
SD means total service downtime within the Agreed Service Time within the relevant Service Period during which a Service and/or part thereof is Unavailable (excluding Planned Downtime, Imposed Carrier Downtime and any Unavailability attributable to Severity 3 or Severity 4 Incidents) within the relevant Service Period.

6.2. Incident Resolution

6.2.1. The Supplier shall ensure that Incidents are resolved within the Maximum Incident Resolution Time.

6.2.2. Maximum Incident Resolution Times are determined by the Severity Levels and Service Maintenance Levels as set out in the following table:

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

Service Maintenance Level	Severity 1; and Severity 2	Severity 3	Severity 4 (Indicative Only)
Level 1	End of next Working Day	5 Working Days	1 Month
Level 2	End of next Working Day	5 Working Days	1 Month
Level 3	Incident reported by 13:00, resolved same day; reported after 13:00, resolved by 13:00 next Working Day	End of next Working Day	15 Working Days
Level 4	6 hours	End of next Working Day	10 Working Days

6.2.3. Each Incident will either be Resolved within the Maximum Incident Resolution Time, or it will not; and will be reported as such by the Supplier. The time taken to resolve the Incident is not material to this Service Level Performance Criteria.

6.2.4. Achieved Incident Resolution is calculated as a percentage of the total number of Incidents in a Service Period that should have been resolved within the Maximum Incident Resolution Time using the following formula:

$$\text{Achieved Incident Resolution \%} = \frac{(\text{TI} - \text{FI}) \times 100}{\text{TI}}$$

Where:

TI means the total number of Incidents raised by the Buyer during the Service Period (excluding Severity 4 Incidents); and

FI means the total number of Incidents raised by the Buyer during the

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

Service Period that were not resolved within the Maximum Incident Resolution Time (excluding Severity 4 Incidents).

6.2.5. Where an Incident is reported outside the Agreed Service Time, the Incident will be treated as if it has been reported at the beginning of the next Working Day.

6.2.6. The Incident will only be deemed to be Resolved once the Services are Available. However, the Supplier shall not formally close any Incident until the Buyer has confirmed that the Services are Available.

6.3. Quality

6.3.1. The Supplier shall ensure that the Services are delivered of a sufficient quality to meet the provisions of this Call-Off Schedule.

6.3.2. Measurement of answer and response times of the Service Desk will be based on the time taken for the Supplier to respond to the Buyer's call or email. Calls and emails receiving an automated response or calls placed into a queuing system shall be deemed not to have been answered.

6.4. Provisioning

6.4.1. The Services will be provisioned at the outset in accordance with any Implementation Plan and any failure to meet Milestones will be dealt with in accordance with the terms of this Call-Off Contract.

6.4.2. Any delivery of Services or part thereof subsequent to the successful conclusion of the Implementation Plan will be subject to the Service Levels identified in the Variation to this Contract that incorporates those changes; or failing any other agreed Service Level, in accordance with the Supplier's standard provisioning Service Levels.

7. Service Credits

7.1. This section sets out the basic agreed formula used to calculate a Service Credit payable to the Buyer as a result of a Service Level Failure in a given Service Period.

7.2. Service Credit payments are subject to the Service Credit Cap.

7.3. Annex 1 to this Part B of this Call-Off Schedule details the Service Credits available for each Service Level Performance Criterion in the event that the

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

applicable Service Level Threshold is not met by the Supplier.

- 7.4. The Buyer shall use the Performance Monitoring Reports supplied by the Supplier under Part C (Performance Monitoring) of this Call-Off Schedule to verify the calculation and accuracy of any Service Credits applicable to each Service Period.
- 7.5. Service Credits are a reduction of the amounts payable in respect of the Services and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in Annex 1 of Part B of this Call-Off Schedule.
- 7.6. The amount of Service Credit is determined by the tables in Annex 1 of this Part B of Call-Off Schedule 14, using the calculated Achieved Service Level Performance Criteria (e.g. Achieved Availability), the Service Level Threshold and the Service Failure Threshold and is calculated by using the straight line formula below:

Service Credit % = $(m \cdot (a - x) + c)$, where

a is the Service Level Threshold (%) below which Service Credits become payable;

b is the Service Failure Threshold (%);

x is the Achieved Service Level Performance Criteria (%) for a Service Period;

c is the minimum Service Credit (%) payable if the Achieved Service Level falls below the Service Level Threshold;

d is the maximum Service Credit (%) payable if the Achieved Service Level Reaches the Service Failure Threshold;

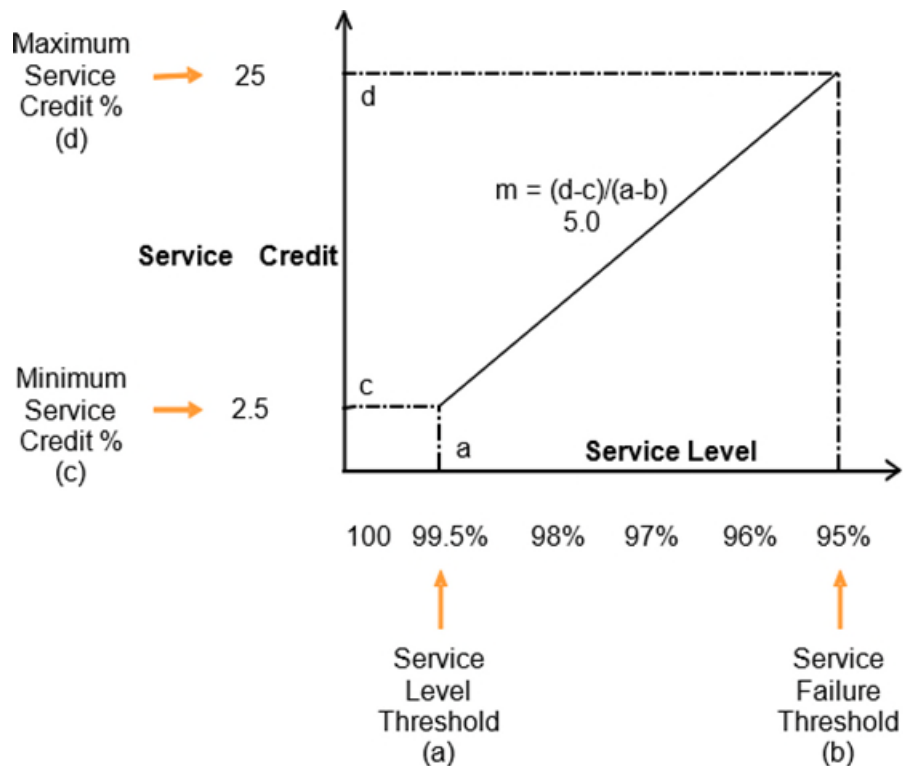
m is a coefficient defined for the services, which is calculated from the Formula $m = (d - c) / (a - b)$, that is the slope of the straight line;

- 7.7. Consequently, the Service Credit regime is shown diagrammatically as follows:

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018



7.8. The Service Credit (£) is subsequently derived as follows:

$$\text{Service Credit (£)} = \text{contract charges} \times \text{Service Credit (\%)}$$

7.9. An example Service Credit calculation for the Availability of a service, (offered herein for illustrative purposes only), is as follows:

Criteria	Coefficient (m)	Service Level Threshold % (a)	Service Failure Threshold % (b)	Minimum Service Credit % (c)	Maximum Service Credit % (d)
Availability	5.0	99.5%	95.00 %	2.5 %	25%

7.9.1. The Achieved Availability of a service was recorded as 97% for a Service Period. For this service, the Service Level Threshold is 99.5% and the Service Failure Threshold is 95%. The contract charges for the service for the Service Period are £3,000. Previous performance had exceeded the Service Level Threshold for Availability.

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

7.9.2. In this illustration example:

$$\text{Service Credit \%} = 5.0 \times (99.5 - 97.0) + 2.5 = 15\%;$$

therefore the Service Credit calculation is:

$$\text{Service Credit (£)} = £3,000 \times 15\% = £450.$$

7.10. An example Service Credit calculation for Incident Resolution is as follows:

Criteria	Coefficient (m)	Service Level Threshold % (a)	Service Failure Threshold % (b)	Minimum Service Credit % (c)	Maximum Service Credit % (d)
Incident Resolution	0.25	95.0 %	85.00 %	2.5%	5%

7.10.1. The Service Level Threshold is 95% of all incidents to be resolved within a specified time with the Service Failure Threshold being 85%. Assume that the Buyer has 80 Incidents within a Service Period, 10 of which were not resolved within the specified time. Therefore, the Achieved Incident Resolution is 87.5% for the Service Period. The contract charges for all the services that the Buyer is consuming are £50,000 per Service Period. Previous performance had exceeded the Service Level Threshold for Incident Resolution Times.

7.10.2. In this illustration example:

$$\text{Service Credit \%} = 0.25 \times (95 - 87.5) + 2.5 = 4.375\%$$

Consequently, the illustrated Service Credit calculation is:

$$\text{Service Credit (£)} = £50,000 \times 4.375\% = £2,187.50.$$

Call-Off Schedule 14 (Service Levels)
Call-Off Ref:
Crown Copyright 2018

PART B Annex 1: Long Form Services Levels and Service Credits Table

1. Availability

1.1. Services (excluding the Service Desk)

Service Maintenance Level	Coefficient (m)	Service Level Threshold % (a)	Service Failure Threshold % (b)	Minimum Service Credit % (c)	Maximum Service Credit % (d)
1	N/A	N/A	N/A	N/A	N/A
2	1.3	95%	80%	5%	25%
3	2.86	97%	90%	5%	25%
4	5	99%	95%	5%	25%

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

1.2. Service Desk

Service Maintenance Level	Coefficient (m)	Service Level Threshold % (a)	Service Failure Threshold % (b)	Minimum Service Credit % (c)	Maximum Service Credit % (d)
All	5	99%	95 %	5%	25%

2. Incident Resolution

Number of Incidents per Service Period	Coefficient (m)	Service Level Threshold %(a)	Service Failure Threshold % (b)	Minimum Service Credit % (c)	Maximum Service Credit % (d)
39 or fewer	Not applicable	No more than 2 Incidents are Resolved in excess of the max Incident Resolution Times	5 or more Incidents are Resolved in excess of the max Incident Resolution Times	2.5% (payable when 3 Incidents breach the Service Level Threshold in any Service Period)	5% (payable when 4+ Incidents breach the Service Level Threshold in any Service Period)
40 and more	0.25	95%	85%	2.5%	5%

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

3. Quality**3.1. Service Desk:**

Criteria	Coefficient	Service Level Threshold	Service Failure Threshold	Minimum Service Credit	Maximum Service Credit
Calls Answered within 60 seconds	0.25	90%	80%	2.5 %	5%
Email Responded to within one (1) Working Day	0.08 3	90%	60%	2.5 %	5%
Abandoned Calls	0.25	95%	85%	2.5 %	5%

3.2. Data Service

3.2.1. Where the Buyer has procured Services that include data services, the following provisions will apply:

- a) The Services will only be deemed to have been Delivered once the Buyer has tested and accepted the quality of the data service;
- b) Subsequent to Services commencement, where the Buyer believes the quality of the data service is not acceptable:
 - (i) an Incident will be raised with the Service Desk
 - (ii) the Supplier shall investigate the Incident;
 - (iii) Subsequent to the investigation, if:
 - A. a fault is found, the Incident is Resolved as any other Incident;
 - B. a fault is not found and the Buyer still believes the quality of the data service is unacceptable, the Supplier shall evidence to the Buyer that the data service complies with relevant Standards.

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

- (iv) In the event that a fault is not found and the Supplier cannot evidence to the satisfaction of the Buyer that the data service complies with relevant Standards, the Service will be deemed Unavailable from the time that the Incident was first raised with the Service Desk and the Incident Resolution Time will be accordingly measured from that time.

3.3. Voice Service

3.3.1. Where the Buyer has procured Services that include voice services, the following provisions will apply:

- a) The Services will only be deemed to have been Delivered once the Buyer has tested and accepted the quality of the voice service;
- b) Subsequent to Services commencement, where the Buyer believes the quality of the voice service is not acceptable:
 - (i) an Incident will be raised with the Service Desk;
 - (ii) the Supplier shall investigate the Incident;
 - (iii) Subsequent to the investigation, if:
 - A. a fault is found, the Incident is Resolved as any other Incident;
 - B. a fault is not found and the Buyer still believes the quality of the voice service is unacceptable, the Supplier shall evidence to the Buyer that the voice service complies with relevant Standards.
 - (iv) In the event that a fault is not found and the Supplier cannot evidence to the satisfaction of the Buyer that the voice service complies with relevant Standards, the Service will be deemed Unavailable from the time that the Incident was first raised with the Service Desk and the Incident Resolution Time will be accordingly measured from that time.

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

PART B Annex 2: Critical Service Level Failure

1. CRITICAL SERVICE LEVEL FAILURE

1.1. A Critical Service Level Failure will be deemed to have occurred if the performance of the Services falls below the same Service Failure Threshold on three (3) occasions in any six (6) consecutive Service Periods.

1.2. In the event of a Critical Service Level Failure, the Buyer shall be entitled to terminate this Call-Off Contract for material Default.

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

Part C: Performance Monitoring

1. Performance Monitoring and Performance Review

1.1. Part C to this Call-Off Schedule provides the methodology for monitoring the provision of the Services:

1.1.1. to ensure that the Supplier is complying with the Service Levels; and

1.1.2. for identifying any failures to achieve Service Levels in the performance of the Supplier and/or provision of the Services (may also be referred to as a "Performance Monitoring System").

1.2. Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.

1.3. The Supplier shall report all failures to achieve Service Levels and any Critical Service Level Failure to the Buyer in accordance with the processes agreed in Paragraph 1.2 of Part C of this Call-Off Schedule above.

1.4. The Supplier shall provide the Buyer with performance monitoring reports ("Performance Monitoring Reports") in accordance with the process and timescales agreed pursuant to paragraph 1.2 of Part C of this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

1.4.1. for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;

1.4.2. a summary of all failures to achieve Service Levels that occurred during that Service Period;

1.4.3. details of any Critical Service Level Failures;

1.4.4. for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;

1.4.5. the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

- 1.4.6. such other details as the Buyer may reasonably require from time to time.
- 1.5. The Parties shall attend meetings to discuss Performance Monitoring Reports ("**Performance Review Meetings**") on a Monthly basis. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:
 - 1.5.1. take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location and time (within normal business hours) as the Buyer shall reasonably require;
 - 1.5.2. be attended by the Supplier's Representative and the Buyer's Representative; and
 - 1.5.3. be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Buyer's Representative and any other recipients agreed at the relevant meeting.
- 1.6. The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Supplier's Representative and the Buyer's Representative at each meeting.
- 1.7. The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

2. Satisfaction Surveys

- 2.1. The Buyer may undertake satisfaction surveys in respect of the Supplier's provision of the Deliverables. The Buyer shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Deliverables which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.

Call-Off Schedule 14 (Service Levels)

Call-Off Ref:

Crown Copyright 2018

PART C ANNEX 1: ADDITIONAL PERFORMANCE MONITORING REQUIREMENTS

Not applicable.

Call-Off Schedule 20 (Call-Off Specification)
Call-Off Ref:
Crown Copyright 2018

Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract

Vodafone IP-VPN

RM6116 - Network Services 3

Service Offer Reference: RM6116-Lot1a-VodafoneLtd-#051

Lot(s): 1a

Effective Date: 12/06/2025

Expiry Date: 20/07/2027



Together we can
vodafone
business

RM6116 Network Services 3

Lot 1a – Inter site Connectivity/Data Access Services

Vodafone IP-VPN

Public Sector



Contents

1.	The Service – Overview and why Vodafone	3
2.	Conditions on the Buyer	3
3.	Outline Implementation Plan	10
4.	Exit Management Plan	10
5.	Service Level Agreement	11
6.	Optional Schedules	16
7.	Mandatory Schedules	16
8.	Service Description and Price Card	17
9.	Ancillary Services	26
10.	Key Sub-Contractors	37
11.	Definitions	38
Appendix 1 – Service Availability		43

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN**

Public Sector

**1. The Service – Overview and why Vodafone**

- 1.1. IPVPN is a secure, private Wide Area Network (WAN) service which supports data, voice, and video traffic virtually over a shared packet network. IP-VPN can be used for point to multi-point or “any to any” wide area communications. IP-VPN is based on a Multi-Protocol Label Switching (MPLS) core, transporting IP traffic.
- 1.2. Vodafone provides you with wide area connectivity for the provision of a managed or unmanaged point-to-point data-only connection and/or point-to-internet/cloud data-only connection (the “Service”).
- 1.3. Our world-class IP-VPN solution meets the needs of small businesses, corporates, government, and multinational organisations. Extensive, local, and international, fixed, and mobile network infrastructure that connects all your sites and workers – and a reliable, secure, and cost-competitive service.

2. Conditions on the Buyer

- 2.1. In the event of a conflict between the terms and conditions included within this Service Offer and the RM6116 Framework or Call-Off terms, then the Framework or Call-Off terms will take precedence.

This Service Offer is available to Buyers that meet and agree to the following criteria:

- 2.2. General Conditions on the Buyer
 - (a) Authorised Users: Access by Buyer to the Services and Equipment is limited to authorised Users. If Vodafone provides each authorised User with User Details, Buyer is responsible for: (a) the security of the User Details; and (b) providing Vodafone with the identity of the authorised Users and keeping that information current. Vodafone accepts no liability for any unauthorised or improper use or disclosure of any User Details. Buyer is liable for all acts and omissions conducted using the User Details up until the time that it informs Vodafone that they are being used without authority or may be compromised.
 - (b) Save as expressly permitted under this Agreement, Buyer shall not resell, distribute, provide or sub-licence the Services or Equipment (except Buyer Equipment) to any third party.
 - (c) Buyer shall take appropriate measures to back up data and otherwise protect against loss of data under this Agreement.
 - (d) Terms of use: Buyer shall not (a) make unauthorised modifications to the Services; (b) use the Services as a means to establish permanent servers, relay connections or interconnection services or any similar commercial activities; (c) do anything that causes the Network to be impaired; (d) use automated means to make calls, texts or send data (including via a GSM Gateway), unless expressly authorised in this Agreement; or (e) use the Services in a way that may reasonably be considered to be a nuisance, defamatory, offensive, abusive, obscene or in violation of any person’s rights or is illegal, fraudulent or contrary to good faith commercial practice to Supplier’s detriment. Buyer shall comply with the AUP in using the Services. Buyer shall notify Supplier immediately of any breach of security or unauthorised use of the Services.
 - (e) Service Monitoring: Buyer gives express consent for Supplier to monitor Buyer’s use of the Service (and disclose and otherwise use the information obtained) only to: (a) the extent allowed by Applicable Law; (b) comply with Applicable Law; (c) protect the Network from misuse; (d) protect the integrity of the public internet and/or Supplier’s systems and Networks; (e) the extent necessary to determine if Buyer has breached any conditions or restrictions on use of the Service; (f) provide the Service; and/or (g) take other actions agreed or requested by Buyer.

RM6116 Network Services 3

Lot 1a – Inter site Connectivity/Data Access Services

Vodafone IP-VPN

Public Sector



- (f) Security: Buyer shall take reasonable steps in line with commercial good practice with entities it controls to: (i) limit misuse of or threat to the Service or Network; and (ii) address any misuse or threat identified by Supplier through the implementation of appropriate security or user controls. Buyer must seek prior approval from Supplier before running any security tests, vulnerability scans or penetration tests on Supplier Equipment or Services.
- (g) Buyer acknowledges that Buyer Equipment not authorised for use on the Network or any unauthorised attempt to repair or tamper with the Equipment may result in an impaired User experience and/or invalidate the manufacturer's warranty.
- (h) Buyer must maintain, install, update and/or follow Supplier's reasonable recommendations regarding Equipment maintenance and/or upgrades.
- (i) Equipment that is (i) out of manufacturer's warranty; or (ii) End Of Life is used at the Buyer's risk unless expressly agreed otherwise by Supplier.
- (j) Buyer shall:
 - (i) Appropriately configure its equipment to enable consumption of the Service.
 - (ii) Maintain Buyer's Equipment.
 - (iii) Provide details to facilitate the delivery, provisioning and billing of the Services requested by Supplier at the time of ordering.
 - (iv) Secure and keep in place, or assist Supplier to obtain (at the Buyer's cost), all relevant third party consents and approvals necessary for the purposes of providing, and preparing for the provision of, the Service. Such consents and approvals include obtaining any necessary wayleave on Supplier's standard terms.
- (k) Termination: Where Buyer terminates the Call-Off Contract during the Call-Off Initial Period, the Buyer agrees to pay Supplier's reasonable and proven losses resulting from the termination of the Call-Off Contract.
- (l) Network Sunset: Buyer hereby acknowledges and accepts that (i) certain Network technologies used to provide the Service on Supplier Equipment or Buyer Equipment may retire prior to the expiry of the contract; (ii) current Networks may be replaced by further advanced Network technologies during the term of the contract. As a result, Buyer agrees that maintaining compatibility of its devices with the available Networks from time to time shall be its responsibility.
- (m) Planned Service changes by Third-Party Providers: Supplier has been informed that BT Openreach (the "Third-Party Provider") for legacy PSTN is withdrawing the service, with full switch off expected to be complete by 31 January 2027. Supplier is entitled to move the Buyer from legacy PSTN to FTTP, SoGEA or Ethernet Access Method as and when required. Buyer will be advised of an alternative Service Element and the associated Charges, as set out in this Service Offer below. Buyer will have the option to either order an alternative Service Element or to cancel the affected Service Element only in accordance with the terms of this Service Offer and Call-Off Contract.
- (n) Format: If Buyer requires this Service Offer (including bills, communications, or any document referred to therein) in a different format, please contact your Vodafone account manager, or frameworks_team@vodafone.com who will clarify Buyer requirements.

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN****Public Sector****2.3. Fixed Services Conditions on the Buyer**

- (a) **Service Commencement Date:** Buyer shall notify Supplier within 5 Vodafone Working Days of the Service Commencement Date if the Services do not conform to Supplier's standard testing criteria and provide sufficient supporting details. Upon receipt of notification, Supplier shall take reasonable action to meet the standard testing criteria.

- (b) **Supplier-Owned Equipment:** The following will apply where Supplier provides Fixed Equipment for Buyer's use with a Service:

- (i) **Title:** Title to the Fixed Equipment at all times belongs to Supplier, its suppliers or subcontractors (subject only to any rights which may be granted to Buyer in respect of Vodafone Software, as set out in this Service Offer).

Buyer Obligations: Buyer agrees to:

- (ii) Provide secure storage for Fixed Equipment that is sent to Buyer Sites prior to installation;
- (iii) Use the Fixed Equipment only for the purpose of using the Services, in accordance with Supplier's instructions and Applicable Law;
- (iv) Allow only Supplier's authorised representatives to add to, move, modify, inspect, test or alter the Fixed Equipment (either on Buyer Site or remotely);
- (v) Adequately insure for, and notify Supplier immediately of loss, breach or suspected breach or damage to the Fixed Equipment;
- (vi) Only connect the Fixed Equipment to the Network using a network termination point that has been approved in advance by Supplier;
- (vii) Provide Supplier with (i) adequate power supply, connection, and space for the operation of the Fixed Equipment at Buyer Sites; and (ii) in the case of BPE patch cords and cabling; and (iii) 10 Vodafone Working Days' notice of any known disruptive event (such as power disconnection). Additionally, specifically in relation to BPE, Buyer shall:
- (A) Appoint a local security representative to ensure the physical security of the BPE who will grant access by approved authorised personnel only and conduct routine physical checks, including ensuring tamper evident labels remain intact; and
- (B) Ensure that the physical environment in which the BPE is housed is appropriate for the protective marking of the data being transmitted through such Fixed Equipment. In particular (i) BPE must be located in a communications room or other isolated area that is suitable to limit the occurrence of accidental or malicious damage to the BPE; and (ii) if the BPE is located in a shared environment, then it must be kept in a dedicated locked cabinet or rack. If that is not possible, robust access control mechanisms must be implemented by Buyer, with access only available with prior approval from Buyer's local security representative.

- (c) **Buyer Equipment:** Where Buyer provides Buyer Equipment for use with a Service Buyer shall (and Buyer acknowledges that failure to do so will excuse Supplier from liability for failure to deliver the Service):

- (i) Install and configure the Buyer Equipment at the Buyer Sites by the date necessary to allow Supplier to perform its obligations;
- (ii) Maintain the Buyer Equipment including prompt installation of security patches and updates;

RM6116 Network Services 3

Lot 1a – Inter site Connectivity/Data Access Services

Vodafone IP-VPN

Public Sector



- (iii) Promptly after the Service terminates, give Supplier access to, and reasonable help with, disconnecting Buyer Equipment from the Service; and
 - (iv) Warrant and undertake that Buyer has full authority to permit Supplier to perform the Services using the Buyer Equipment.
- (d) Buyer Sites: for the purposes of preparing for and delivery of the Services, Buyer shall:
 - (i) Carry out, or permit Supplier or its subcontractors to conduct, a Site Survey;
 - (ii) Prepare the Buyer Site for the Services in accordance with Supplier's instructions;
 - (iii) Allow and/or have in place (or assist Supplier to do so at Buyer's cost) all third party consents necessary to allow Supplier or its subcontractors and agents (and obtain consents from third parties to allow) to:
 - (A) Access the Buyer Sites, and any Buyer Equipment, Fixed Equipment or Equipment, and third-party property located there, as Supplier reasonably requires to perform its obligations under this Agreement (including for the purposes of installing and uninstalling Equipment (whether in the Buyer Sites or outside) and providing and preparing for the provision of, the Services) and including access outside Working Hours; and
 - (B) Ensure that Buyer Sites are safe and have a suitable working environment.
- (e) Emergency Services:
 - (i) General: In the event of a power cut or failure affecting Buyer's fixed line and/or broadband Service, and/or a failure of the internet connection on which the Service relies, Buyer may not be able to make calls including calls to emergency services. This may also affect any calls using the internet including calls to emergency services.
 - (ii) Buyer obligations: Buyer shall:
 - (A) Provide Supplier with complete and accurate Buyer Site address information; and
 - (B) Give Supplier at least 30 days' written notice of any change to the location of any Fixed Equipment and to any change to the relevant Buyer Site address information.
 - (iii) Buyer acknowledges that any failure to provide the information required in 2.3(e)(ii) may render emergency services unable to identify User's location.
 - (iv) Calls using the internet: where a Service places calls using the internet, Buyer shall:
 - (A) Make Users accessing the Service via a soft client aware that Supplier may be unable to automatically determine their location if they make an emergency services call using the Services; and
 - (B) Ensure that such Users provide their location details in the event that they make an emergency services call using the Services. In the event of a power failure, the emergency call placed will be routed over the Network and not through the Service.
 - (C) Provide a registered address where a Buyer or User will make calls over the internet including if there are multiple addresses where such calls will be made and keep information on all such locations up to date.
- (f) Survey: This Service Offer and each Service Element is subject to survey. In the event a Site Survey output results in an increased price from the Call-Off Contract, the Buyer has the right to cancel the affected Service Element only in accordance with the terms of this Service Offer and Call-Off Contract.

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN****Public Sector**

- (g) Unless otherwise agreed and stated in the Buyer's Call-Off Contract, the Buyer will be liable for any additional costs charged to Supplier by third parties in connection with the provision of the Services. Such Charges (often referred to as Excess Construction Charges) are detailed in the Ancillary Services section of this Service Offer. These Charges will be notified to the Buyer before any construction works take place. In the event this results in an increased price from the Call-Off Contract, the Buyer has the right to cancel the affected Service Element only in accordance with the terms of this Service Offer and Call-Off Contract.

2.4. Tiered Support Services conditions on Buyer

- a) Buyer shall:
- i) Nominate, and notify Vodafone of, one or more points of contact with contractually binding authority to be the primary management interface between Buyer and Vodafone and enable Vodafone's delivery of Tiered Support Services;
 - ii) Provide Vodafone with an email address for day-to-day correspondence and notify of any changes; and
 - iii) Maintain a Buyer's Service Desk as the initial point of contact between Vodafone and the Buyer for any suspected or reported Incidents.
- b) Buyer shall ensure it:
- i) Provides Vodafone with a key site list of all Buyer Sites that should be prioritised in the event of a BMI ("Key Sites") by the Service Commencement Date; Only 10% of the total Buyer Sites can be identified as Key Sites, e.g., if the Buyer has 17 sites, 2 can be Key Sites.
 - ii) Notifies Vodafone of any updates or amendments to the Key Site list during the Contract Period by email to the appointed service manager at Vodafone; and
 - iii) Carries out an initial analysis of any Incident reported to its Buyer's Service Desk, to establish whether the Incident should be referred to Vodafone.

2.5. IP-VPN Conditions on the Buyer

- a) Buyer shall not (and shall ensure that its Users shall not) connect or seek to connect the Services to the public switched telecommunications network (PSTN) otherwise than in accordance with Applicable Law.
- b) The services under this Service Offer are available to Buyer Sites located on the UK mainland (England, Scotland, and Wales) and Northern Ireland.
- c) The services are supplied in accordance with the Vodafone Acceptable Use Policy, and Recovery Policy which are available on request.
- d) The Buyer shall at the time of ordering any of the Services under this Service Offer:
- i) Provide full details of the Services required and the Buyer site locations to enable validation of the Call-Off Contract. Such details shall include:
 - A) Access and/or Service Bandwidth required
 - B) Rack location
 - C) Room name or room number
 - D) Building name, number, and floor.
 - E) Street name, town, city & postcode
 - ii) For each Buyer Site location, the Buyer shall provide a site contact name and contact details to include:
 - A) Contact telephone and email address
 - iii) provide 10/100/1000 Mbit/s Ethernet (IEEE802.3/IEEE802.3u) LAN port and RJ45 cable to connect to the BPE router or alternative interface agreed at time of order

RM6116 Network Services 3

Lot 1a – Inter site Connectivity/Data Access Services

Vodafone IP-VPN

Public Sector



- e) Where the services are to be provisioned at a Buyer site that is owned by a third-party landlord the Buyer shall advise the landlord or site owner's details including:
 - i) Landlord or site owner company name
 - ii) Name of nominated representative, including contact details
 - iii) Landlord or site owner building address including:
 - A) Room name and/or room number
 - B) Building name, number, and floor.
 - C) Street name, town, city & postcode
- f) The Buyer shall provide full details to enable billing of the Service including:
 - i) Billing contact name, telephone, and email contact details
 - ii) Purchase order references
 - iii) Billing entity/company name
 - iv) Billing address
 - v) VAT Registration Number
- g) Appropriately configure its equipment to enable consumption of the Service;
- h) Maintain its own equipment;
- i) PSTN and IP Voice / Video services: Buyer acknowledges that the Service is not a public voice service. Buyer and its Users shall not connect or seek to connect the Service to any public voice service, including the public switched telecommunications network (PSTN) or other voice or video services (e.g., voice over IP) unless Buyer purchases such services from Vodafone or Buyer is permitted to connect the Service to a PSTN in accordance with Applicable Law.
- j) Public Internet service: Buyer acknowledges that the Service is not a public Internet service. Buyer and its Users shall not connect or seek to connect the Service to a public Internet service and/or enable the use of public Internet for any voice or video communication service (e.g., voice over IP), unless Buyer purchases public internet service from Vodafone or Buyer is permitted to connect the Service to a public internet service in accordance with Applicable Law.
- k) Security Obligations: Buyer will: (a) design, implement, manage, and archive configuration of internal IP protocols, LAN information and access lists; (b) provide reasonable security on the Equipment and Buyer's private networks to limit misuse of or threat to the Service, Equipment or Network;(c) address any misuse or threat identified by Vodafone through the implementation of further security or user controls.
- l) Classes of Service: If Vodafone does not provide a Buyer Premise Equipment (BPE) Router, Buyer is responsible for configuring the Buyer's Router in accordance with the relevant CoS codes. Failure to do so will prevent the CoS profile from working and Vodafone shall have no liability in respect of such a failure.
- m) Buyer may propose a change to the Service by written request ("Service Change Request Procedure"). Upon agreement, the Parties must authorise the change in the form of a change Order or other written amendment to the Agreement (a "Change Order"). Vodafone has no obligation to commence work in connection with a change until a Change Order is executed by the Parties. If it is necessary to use additional resources or to incur any other additional costs in making a change, they shall be calculated as a change to the Charges.
- n) Regulated Items: The use, export, and/or import of certain Equipment are subject to Applicable Laws ("Regulated Items"). Buyer must only deploy, export, import, and/or disclose Regulated Items in strict

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN****Public Sector**

compliance with all Applicable Laws, and specifically Applicable Laws regarding encryption. If Applicable Law prohibits the export, re-export, import, and/or use of a Regulated Item in certain jurisdictions, that prohibition may preclude the use of the Service in those jurisdictions.

o) Simple Network Management Protocol:

- i) Vodafone may withdraw the SNMP if: (a) in Vodafone's opinion, it represents a potential or actual security risk to the Services; (b) it is used by the Buyer in a way which constitutes a breach of the Agreement or results in a breach by Buyer of the SNMP read-only access service security; or (c) in Vodafone's reasonable opinion, it prevents further enhancements to Vodafone's services, including but not limited to the Services.
- ii) If Buyer's use of the SNMP read-only access Service deliberately, negligently, or recklessly causes an impact on Network or device performance, Buyer shall be liable for the costs incurred by Vodafone for rectifying the problem.

p) DSL and GPON: Where any Buyer Sites are connected to the Backbone by an access circuit using DSL, GPON or SISA utilising DSL or GPON the following shall apply:

- i) Pre-sales availability checks are not an absolute guarantee that the access method, or specific variant, can be provided.
- ii) The provision of the Service is conditional upon confirmation from any third-party supplier to be used in connection with the Service that it is able, and agrees, to provide the access method and, if relevant, installation and/or survey services, at the relevant Buyer Site.
- iii) Where an ordered access circuit or service, cannot be provided, Vodafone will advise Buyer of alternative options and Charges. Buyer may order an alternative or cancel such service or access circuit, without incurring an applicable Recovery Charge.
- iv) Where Buyer Sites are connected by DSL or GPON, Vodafone shall inform Buyer of the date of the Buyer Site visit but may not confirm an exact time.
- v) Due to ongoing technical advances and the replacement of copper access infrastructure by Passive Optical Networks, DSL may become obsolete during the contract term. Vodafone may replace any DSL access with GPON access at its discretion. An additional charge maybe levied to connect to GPON.
- vi) Services are asymmetrical in nature with bandwidth from the network to the Buyer site far higher than the Buyer site to the network, typically between 5:1 and 10:1 difference.

q) Ethernet Access:

- i) Where dual access is provided using third party access circuits, Vodafone cannot guarantee end-to-end diversity of the access circuits.
- ii) Where an access circuit ordered cannot be provided at a Buyer Site, Vodafone will advise Buyer of alternative options and Charges. Buyer may order an alternative or cancel, without incurring an applicable Recovery Charge.

r) Secure Internet Site Access:

- i) Where Secure Internet Site Access is ordered by the Buyer as an access method, Vodafone will provide access to the Service via an encrypted tunnel over a local in-country public internet access service.

2.6. Secure Network Gateway conditions on the Buyer

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN****Public Sector**

- a) Buyer shall provide Vodafone with accurate and up to date information relating to the configuration of the policies associated with the firewall throughout the initial period.
- b) While SNG Service is designed to prevent outsiders from gaining access to the IP-VPN and provides an effective method of monitoring and limiting access, it may not prevent some instances of unauthorised access to the IP-VPN.
- c) Buyer understands that the SNG service is a layer 1-4 service only and does not provide application level aka layer 7 scanning or inspection.

3. Outline Implementation Plan

- 3.1. Supplier provides you with a comprehensive service, moving the Buyer from the Service Commencement Date as per the Call-Off Contract to Buyer's first bill. Supplier's outline Implementation Plan is detailed below, and will be updated to become the draft Implementation Plan once the Call-Off Contract has been received by Supplier:
- i) Supplier will validate the Call-Off Contract containing the details of the Services being implemented under this Service Offer.
 - ii) Supplier will confirm the Call-Off Contract with a representative from the Buyer's organisation advising of any missing details.
 - iii) Once all details are provided by the Buyer, Vodafone will submit the order for delivery and advise the Service Commencement Date to the Buyer.
 - iv) Supplier will manage the intermediate activities supporting the implementation process.
 - v) Supplier will conduct end-to-end testing and confirm to the Buyer when the Service is ready for use.

4. Exit Management Plan

- 4.1. Whether the Buyer would like to cease or move their services to a new provider entirely, Vodafone's Exit Management plan is outlined below;
- a) The Buyer will notify Vodafone of its plan to cease or migrate away from any service within the minimum termination period agreed within the call off-contract.
 - b) Vodafone will extract a contract end date report which will detail the current account set up and any applicable termination fees that will apply to the Buyers final invoice.
 - c) Upon formal request from the Buyer, Vodafone, where applicable, will generate relevant authorisation/decommissioning codes within the regulatory time period.
 - d) The Buyer will manage their relationship and migration plan with their new supplier and, if applicable, share any relevant data provided by Vodafone to their new supplier

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services**

Vodafone IP-VPN

Public Sector

**5. Service Level Agreement**

5.1. For the purposes of this Service Offer:

- a) The provisions of this Service Level Agreement are compliant with the Service Maintenance Level 1 as set out in Schedule 14 of the Call-Off Terms.

Vodafone Tiered Support Service Model

- a) In addition to the Service Level Agreement in Service Maintenance Level 1 as set out in Schedule 14 of the Call-Off Terms the Buyer will also benefit from the following additional Tiered Support Service Model ("TSSM") as part of the Service,

- i) Service Request Fulfilment Support Services:

- A) Response and Acknowledgement

Deliverable	Contact Method	SLT
Vodafone Initial Response	Email	Near Instant

- ii) Incident Management Support Services:

- A) Incident Management Response and Acknowledgement:

Deliverable	Contact Method	SLT
Vodafone will provide the means to report an Incident and provide an Initial Response by the same means.	Telephone	90% of calls answered <20 seconds

- iii) Incident Management Diagnosis:

Deliverable	Contact Method	SLT
Following an Initial Response and as part of initial diagnosis, Vodafone will: (a) determine the Infrastructure Service or Supported System on which the incident has occurred; and (b) determine the perceived impact and urgency of the incident including assessment against the criteria for a BMI Vodafone will route the Incident Record to the appropriate support function for expert diagnosis and subsequent management.	Telephone	<30 minutes
Vodafone will contact the party raising the incident to confirm Resolution and closure.	Telephone	<24 hours from Resolution
Vodafone will provide incident updates for each Impact 1 Incident	Telephone	Initial update within 1 hour. Thereafter minimum of hourly or as agreed
Vodafone will provide incident updates for each Impact 2 Incident	Telephone	Initial update within 1 hour. Thereafter minimum of hourly or as agreed

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN****Public Sector**

iv) Buyer Major Incident Management

Deliverable	Contact Method	Premium SLT
Vodafone will attend a conference call on request for a BMI that is in progress	Telephone	15 minutes from receipt of request (subject to the Buyer Site being included in the key site list).
Vodafone will provide enhanced structured Incident updates for BMIs	Telephone	Initial update ≤1 hour, minimum of every 30 minutes thereafter or as agreed
Vodafone will provide a BMI high level executive summary, after the Incident is resolved	Telephone	2 Working Days
Vodafone will provide a full BMI report, after RCA of the Incident has been resolved	Telephone	5 Working Days
Volume of Buyer Sites that require BMI	Telephone/email	10% of Buyer Sites

v) Financial Management (Billing) Support Services:

A) Billing Queries:

Deliverable	Contact Method	SLT
Vodafone will provide the means to raise billing queries and provide an Initial Response via email	Email	Near Instant
Vodafone will ensure that all billing queries received via email are Acknowledged	Email	<24 hours

B) Performance Reports

Deliverable	Enhanced SLT
Vodafone will provide scheduled account billing reviews.	Quarterly

vi) Operational Change Management Support Services

- A) A Vodafone-designated “Change Manager” will be responsible for changes and the change management process established by Vodafone from time to time. The Change Manager may be from Vodafone, Buyer or a third party, dependent upon where Vodafone (acting reasonably) determines that responsibility for change governance resides.

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN****Public Sector**

B) Notification of Planned and Essential Operational Changes:

Deliverable	Contact Method	SLT
Vodafone will provide notification of a Planned Outage	Email	10 Working Days
Vodafone will notify Buyer in advance, where reasonably possible, of the scheduling of an Essential Outage	Email	>48 hours

C) Change Schedule Provision

Deliverable	Contact Method	Enhanced SLT
Vodafone will provide and maintain a Change Schedule	Email	Weekly

D) Change evaluation and Support

Deliverable	Contact Method	Enhanced SLT
Vodafone will ensure that all normal operational changes proposed by Buyer, to be delivered by Vodafone are evaluated against the Service referred to in the request by the Buyer and not against multiple Services (unless expressly requested by the Buyer), as provided by Vodafone under the Call-Off Contract to ensure risks have been managed.	Telephone and email	No SLT

vii) Problem Management Support Services

A) Initial Response, Acknowledgement and Routing

Deliverable	Contact Method	Premium SLT
Vodafone will provide the means to report a Problem and provide an Initial Response by the same means.	Email	Near Instant
Vodafone will validate the request for a Problem Record. If the request is valid create a Problem Record and provide an Acknowledgment.	Email	95% <4 Working Hours from receipt
Vodafone ensure all Problems are routed to the appropriate technical or problem management team for Resolution	N/A	No SLT

B) Problem Root Cause Analysis ("RCA") Requests

Deliverable	Contact Method	Premium SLT
Vodafone will carry out RCA on all Impact 1 Incidents	N/A	95% <20 Working Days
Vodafone will carry out Buyer specific basic trend analysis of closed Incidents	N/A	Service not available
Vodafone will carry out Buyer specific in-depth trend analysis of closed Incidents	N/A	No SLT
Vodafone will coordinate RCA investigation of BMIs	N/A	90% <10 Working Days

C) Problem and Incident Trend Analysis Reporting and Review

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN****Public Sector**

Deliverable	Contact Method	Premium SLT
On request Vodafone will provide an initial problem analysis report for those Impact 1 incidents that have repeated 3 times in any 28 day period.	Email	5 Working Days
On request Vodafone will provide an Incident RCA report which includes either the root cause found or an action plan to determine the root cause where reasonably possible for Impact 1 incidents that have repeated 3 times in any 28 day period.	Email	5 Working Days
As part of the “enhanced problem management reports pack” Vodafone will provide a high level trend analysis report.	Email	Service not available
As part of the “premium problem management reports pack” Vodafone will provide a low level trend analysis report.	Email	Monthly
As part of the “enhanced problem management reports pack” Vodafone will provide a Problem Record status report.	Email	Service not available
As part of the “premium problem management reports pack” Vodafone will provide a Problem Record status report.	Email	Weekly

D) Problem Management reviews: Problem and Incident Trend Analysis and Reporting

Deliverable	Contact Method	Premium SLT
Vodafone will provide Problem Record status report review meetings (the problem status report review meeting will only take place if there are any open cases).	Telephone	Weekly

viii) Service Level Management

A) Performance Reports

Deliverable	Contact Method	Premium SLT
Vodafone will create mid-level reports detailing the report's format, content and SLT performance for publication of those reports for each Service that Vodafone provides	Portal/Email	Service not available
Vodafone will create in-depth Reports detailing the report's format, content and SLT performance for publication of those reports for each Service that Vodafone provides	Portal/Email	No SLT

B) Vodafone Service Level Management Team

Deliverable	Contact Method	Premium SLT
Vodafone will provide analysis of performance reports to identify trends, and areas for improvement in the Infrastructure Services and Tiered Support Services being provided and reported on.	N/A	10 Working Days after Reporting Period
Appropriate findings resulting from analysis will be addressed in a service development plan.	N/A	Quarterly
Vodafone will provide performance review meetings with Vodafone service management resource.	Telephone	Service not available
	In person	Monthly

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN**

Public Sector



Deliverable	Contact Method	Premium SLT
Vodafone will either itself or via an independent third party continually measure Buyer satisfaction with interactions from a sample of all customers	Telephone (third party to Buyer)	Service not available
	Telephone	Quarterly
Vodafone will provide service improvement plans as are reasonably required to facilitate improvement where it is needed (at Vodafone's discretion, acting reasonably).	N/A	No SLT
Vodafone will maintain and update a customer support services handbook as it deems required.	N/A	Quarterly
Vodafone will work with Buyer to produce and maintain a service development plan.	N/A	Quarterly

C) Business Relationship Management

Deliverable	Contact Method	Premium SLT
Vodafone will provision regular sector review meetings with a senior manager and Buyer's account manager	In person	Quarterly
Vodafone will provision regular futures review meetings with its nominated subject matter expert(s), senior operational manager(s) and Buyer's account manager	In person	Bi-annually
Vodafone will provision and maintain a risk register relating to Services provided by Vodafone under these Tiered Support Service Specific Terms and conduct regular reviews and analysis of the risk register with Buyer	In person	Bi-annually

ix) Service Request Catalogues

- A) Vodafone may make one or more "Service Request Catalogues" available to Buyer through its online portal at OnePortal ("Portal"). A URL for the Portal will be provided to the Buyer via the support handbook. Service Request Catalogues contain information about the Tiered Support Services and Service Requests, including those Service Requests that will be self-served by the Buyer and those that will be serviced by Vodafone, broken down by Service.
- B) Any Service Request Catalogue information made available to Buyer is provided for guidance only; it is not binding on Vodafone and does not form part of this Agreement.
- C) Vodafone may change the information contained in the Service Request Catalogue at its discretion, via a catalogue update, provided that the changes do not materially affect the nature of the Tiered Support Services delivered to Buyer.

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services**

Vodafone IP-VPN

Public Sector

**6. Optional Schedules**

This Service Offer assumes that the Buyer is not electing to take any of the following Optional Schedules;

- 6.1. Call-Off Schedule 4 of the Call-Off Contract shall not apply.
- 6.2. Call-Off Schedule 6 of the Call-Off Contract shall not apply.
- 6.3. Call-Off Schedule 7 of the Call-Off Contract shall not apply.
- 6.4. Call-Off Schedule 10 of the Call-Off Contract shall not apply.
- 6.5. Call-Off Schedule 13 of the Call-Off Contract shall not apply.
- 6.6. Call-Off Schedule 15 of the Call-Off Contract shall not apply.
- 6.7. Call-Off Schedule 16 of the Call-Off Contract shall not apply.
- 6.8. Call-Off Schedule 17 of the Call-Off Contract shall not apply.
- 6.9. Call-Off Schedule 18 of the Call-Off Contract shall not apply.
- 6.10. Call-Off Schedule 22 of the Call-Off Contract shall not apply.
- 6.11. Call-Off Schedule 23 of the Call-Off Contract shall not apply.
- 6.12. Call-Off Schedule 24 of the Call-Off Contract shall not apply.
- 6.13. Call-Off Schedule 25 of the Call-Off Contract shall not apply.
- 6.14. Joint Schedule 6 of the Call-Off Contract shall not apply.
- 6.15. Joint Schedule 7 of the Call-Off Contract shall not apply.
- 6.16. Joint Schedule 8 of the Call-Off Contract shall not apply.
- 6.17. Joint Schedule 9 of the Call-Off Contract shall not apply.
- 6.18. Joint Schedule 12 of the Call-Off Contract shall not apply.

Should the Buyer wish to take any of the above schedules, then these may be subject to additional charges. Please contact your Vodafone account manager, or frameworks_team@vodafone.com who will clarify your requirements, and where needed publish a new Service Offer containing the selected Optional Schedules.

7. Mandatory Schedules

- 7.1. In accordance with the Supplier's obligations under any Call-Off Contract, Vodafone has developed and will maintain the following reports and plans, which are available to view, download, print or save, on Vodafone's Public Sector Portal. By entering into a Call-Off Contract Buyer confirms that it accepts the following reports and plans as is, with no alteration:
 - a) Call-Off Schedule 1 (Transparency Reports) - Transparency Report in accordance with Call-Off Schedule 1.
 - b) Call-Off Schedule 8 (Business Continuity and Disaster Recovery) – Business Continuity and Disaster recovery Plan in accordance with Call-Off Schedule 8.

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN****Public Sector**

- c) Call-Off Schedule 9 (Security) - Security Management Plan in accordance with Call-Off Schedule 9. The Buyer hereby acknowledges and agrees that the Supplier's Security Management Plan is incorporated in Part A of Call-Off Schedule 9. . By entering into a Call-Off Contract the Buyer acknowledges and agrees:
 - i) the Supplier has prepared and delivered the Security Management Plan to the Buyer; and
 - ii) the Buyer has approved the Security Management Plan, in accordance with Call-Off Schedule 9 (Security) Part A: Short Form Security Requirements.

8. Service Description and Price Card

8.1. Primary Services

IP-VPN is a secure, private Wide Area Network (WAN) service which supports data, voice, and video traffic virtually over a shared packet network. IP-VPN can be used for point to multi-point or "any to any" wide area communications. IP-VPN is based on a Multi-Protocol Label Switching (MPLS) core, transporting IP traffic.

The service enables the Buyer to establish a private wide area network to underpin critical communications. An IP Virtual Private Network (VPN) is built and configured between various nominated Buyer Sites, which are connected to the Vodafone IP-MPLS Network using a range of site topologies and network access methods to meet availability and performance requirements.

The IP-VPN Service provides the Buyer with data connectivity between Buyer sites and enables the sharing of data services between each of the connected sites. If the Buyer requires any technical information beyond the scope of this Service Offer in relation to the Vodafone IP-VPN service, a technical specification can be made available on request by contacting your Vodafone account manager, or frameworks_team@vodafone.com.

- a) The main service components of the IP-VPN service are:
 - i) Access circuit – this connects a Buyer Site to a port on Vodafone's MSP network. The port bandwidth can be throttled allowing the Buyer to pay only for the service bandwidth which it needs. Backup and Resilience options are also supported.
 - ii) Class of Service (QoS) – the IP-VPN service supports the standard six (6) traffic differentiation classes on all Ethernet access types (not available on ADSL16 and FTTC Elevated 40/10). These are summarised in the below table
 - iii) Buyer Premise Equipment (BPE) (i.e. Router) – The service can be provided on a wires-only basis or inclusive of managed Buyer Premise Equipment router hardware
 - A) If the Vodafone Supplied Router becomes unsupported by the manufacturer, Vodafone may replace the Vodafone Supplied Router with an equivalent supported router at Vodafone's discretion.
 - B) BPE are specified and tested up to a recommended maximum throughput. The Buyer must specify a BPE who's maximum throughput is higher than the service speed called off.
 - iv) Service and support on a 24x7x365 basis with proactive monitoring (Severity Level 1-2 Incidents) and 24/7 Incident Management; including interface down, BGP routing failure, bouncing interfaces, unreachable device.
- b) Optional features of the IP-VPN service are:
 - i) Network Based Internet Access and network-based Firewall including Secure Network Gateway – access to the Internet from within the network securely

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN****Public Sector**

- ii) Secure Internet Site Access – a remote access connectivity to your IP-VPN network for users or 3rd parties working at a specific remote location
- iii) Cloud Connect – access to centralised cloud-based applications from within your IP-VPN network hosted within cloud providers such as Amazon, Google, and Microsoft.

Quality of Service classes and recommended use.

The IP-VPN service supports differentiation of traffic across the network by the application of Quality of Service. The six classes available are shown below. A service can consist of a single class; two classes or more or all classes on the same site connection and network as befits the Buyer requirements

Note: not all Class of Service levels are available where access uses DSL, GPON or SISA.

The VPN port bandwidth Annual Recurring Charge defined under this Service Offer is for Default class bandwidth. Charges for other traffic classes are detailed section 8.15 and are in addition to the VPN port bandwidth Annual Recurring Charge.

Class of Service	Description	Typical Applications	Application Characteristics
Premium	The highest-level CoS, prioritised over all other traffic.	Voice, Video Conferencing	Real time, business critical, designed for voice.
Enhanced 1 Enhanced 2 Enhanced 3	Three Enhanced classes to enable separation of different types of critical traffic.	Enterprise applications such as Citrix, Oracle, SAP. Financial transactions, streamed video. Allocating applications to an Enhanced CoS can protect them from high-bandwidth, low-priority traffic such as FTP and HTTP downloads.	Important, interactive, less sensitive to jitter but still delay sensitive.
Standard		Email, web browsing, FTP, HTTP downloads.	Not real time or interactive. Not sensitive to jitter or delay but more important than reasonable efforts traffic (Default Class)
Default	The lowest-level CoS.	Email, web browsing, FTP, HTTP downloads.	Not real time or interactive. Not sensitive to jitter or delay

Additional default class traffic is selected by choosing the relevant VPN port bandwidth. Standard class is charged at the same rate as default class and where required must be stated at time of order.

- c) The Charges payable in respect of this Service are set out in the Price Card below.

The Charges for single circuit are made up of:

- i) Set up/Installations Fee (One Off)
- ii) Annual recurring charges (billed either monthly or annually)
- iii) Modification Charges (where requested by the Buyer);
- iv) Professional Services (if applicable)
- v) Support Service (if applicable)
- vi) Optional Managed Router (this is where Vodafone will provide proactive management and maintenance of the Vodafone provided router)

- d) All pricing is based on either a 12-month, 24-month, or 36-month initial period.

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN****Public Sector**

- e) Buyer Premise Equipment (BPE) – where optional managed routers are chosen by the Buyer, the routers will be installed, configured, managed, and maintained by Vodafone. There are two types of BPE a Buyer can purchase;
 - i) Standard – Router hardware capable of supporting the requested VPN (port) throughput bandwidth as measured using an IMIX traffic profile.
 - ii) Premium – Router hardware capable of offering a higher service performance and supporting upgrades in VPN (port) bandwidth without a change in router hardware. Premium router hardware shall be capable of supporting the maximum VPN (port) bandwidth possible on the chosen access connectivity based on a IMIX traffic profile. Premium router hardware should be selected where there is a requirement for a small average 64 Byte packet size (such as for large IP Voice traffic usage)
- f) Enhanced Network Performance Service reporting – where ordered, reporting options are available which give greater visibility of service performance adding Latency, Jitter and Packet loss visibility between selected Buyer sites. Vodafone IP-VPN Online Performance Reporting (OPR) provides you the visibility required to plan, deploy, ensure, troubleshoot, and optimise complex WAN environments and applications. It empowers your IT organisation with the real-time technical insight and business relevant performance metrics needed to guarantee end-user satisfaction and productivity. Capability offered includes:
 - i) Global Dashboard With a Summary of Site Inventory
 - ii) Detailed Site Inventory
 - iii) Planned Outage notifications Dashboard Network Performance Reporting

[REDACTED]



[REDACTED]

[REDACTED]

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

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

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

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

Enhanced Class of Service allows for prioritisation of delay-sensitive traffic through the implementation of traffic classification (the 'marking of traffic') at the network edge for carriage across the service.

- [illegible]

RM6116 Network Services 3

Lot 1a – Inter site Connectivity/Data Access Services

Vodafone IP-VPN

Public Sector



h) Premium Class of Services (CoS)

Premium Class of Service allows for prioritisation of delay-sensitive traffic through the implementation of traffic classification (the 'marking of traffic') at the network edge for carriage across the service.

- Class of Service (COS) is priced based on the percentage of Standard VPN Port Bandwidth required as Enhanced or Premium COS
- Use the Matrix to select the COS Price. All Prices are ARC
- Select Standard VPN Port in the Vertical Column and scroll Horizontally to the required Premium COS Bandwidth
- Premium and Enhanced COS Prices are in addition to Standard VPN Port Pricing.

Cloud Connect provides private connectivity to Cloud Provider Data Centre directly from the IP-VPN Network, for improved security, performance and availability compared to using the public Internet. Cloud Connect provides the following capabilities:

- Consistent, committed bandwidth at rates from 50Mbps to 1Gbps allowing Network capacity to scale as required.
- Flexible contract duration from one month to sixty months.
- Includes dual access from two PEs to a Cloud Provider Data Centre for high availability.
- Secure private connections ensure the Buyer's traffic is segregated.
- Authorisation of connections maintains the confidentiality and integrity of information.
- Connectivity to Cloud Provider Data Centre locations in different regions reduces latency and aids compliance with data residency and data sovereignty requirements.
- Managed service including ordering, support, escalations, reporting and ticketing (as for IP-VPN).

RM6116 Network Services 3

Lot 1a – Inter site Connectivity/Data Access Services

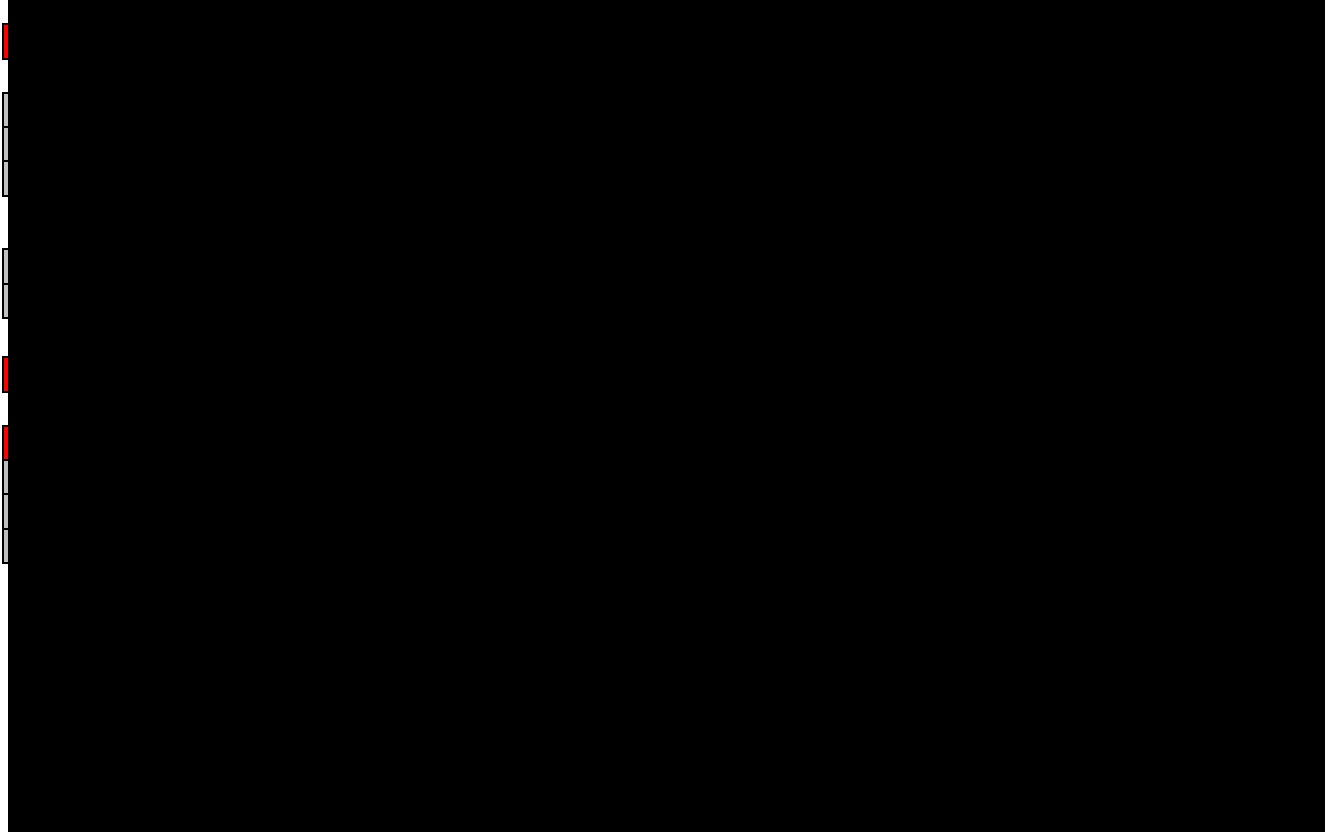
Vodafone IP-VPN

Public Sector



8.2. Technology, Equipment and Solutions

Additional Services



RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN****Public Sector****Enhanced Network Based Internet Access (NBIA)**

Enhanced NBIA provides Users at any Buyer Site on a Buyer's IP-VPN with a central public Internet gateway facility. The Enhanced NBIA service by default comes with a basic ruleset to allow outbound but restrict inbound access. This default firewall will provide the minimum level of security and suits simple web browsing use cases for Enhanced NBIA. For greater granularity of control, and to allow additional features such as application reporting, then Vodafone can provide a range of Firewall options that increase in functionality to a fully managed, premium, firewall option.

Buyer's use of Enhanced NBIA is limited to the following countries at time of contracting:

Vodafone Licenced Countries		
Austria	Hong Kong	Portugal
Australia	Hungary	Russia
Belgium	Italy	Singapore
Canada	Ireland (Republic of)	South Korea
Czech Republic	Japan	Spain
Bulgaria	Luxembourg	Sweden
Denmark	Malaysia	Switzerland
Finland	Mexico	Ukraine
France	Netherlands	UK
Germany	Norway	USA

Secure Network Gateway:

SNG is ordered with Enhanced NBIA. Buyer may order a range of firewall and security features under the Standard and Premium packages set out below. SNG Service includes a network-based firewall facility. If ordered, Vodafone will consult with Buyer to capture preferred security rules and configuration requirements.

(i) The following Standard and Premium feature sets are available:

Items	Standard	Premium
Inbound/outbound ruleset	Up to 50	Up to 1000
Application reporting	Yes –	Yes -
Firewall event/logs	6-month retention	12-month retention
Reports frequency	weekly/monthly	Daily/weekly/monthly

(ii) Additional options for intrusion Detection and Prevention are set out below:

Items	Standard	Premium
Policy protection	Default	Customisable
Threat detection via SSL	No	Yes
Anomaly based detection	No	Yes - with tuning support
NIDs/NIPs events/logs	6-month retention	12-month retention
Reports frequency	weekly/monthly	Daily/weekly/monthly

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services**

Vodafone IP-VPN

Public Sector



✕ = Not Available ✓ = Included in Package ● = Optional Add-on (Additional Charge)		Firewall Type (Package)		
Description	Features	Default (Enhanced NBIA Only)	Standard Firewall	Premium Firewall
Enhanced NBIA Only Default ruleset for Enhanced NBIA – allowing all outbound access with PAT to single public address Fully Managed Enhanced NBIA with Firewall service to support outbound & inbound security policies.	Ruleset allowing all outbound traffic	✓	✕	✕
	Ruleset preventing all inbound traffic			
	Inbound and outbound rulesets and	✕	✓ Up to 50	✓ Up to 1000
	Change Management through Vodafone service desk	✕	✓	✓
	Firewall event/logs for downloading within Vodafone portal (6-month retention)	✕	✓ 6 months log retention	✓ 12 months log retention
	Firewall reports - Ability to view, & download (or email) reports via Oneportal	✕	✓	✓
	DMZ deployment for public facing applications (recommended for inbound access from internet)	✕	● Optional Add-on	● Optional Add-on
	External Syslog feed (for 3rd party)	✕	● Optional Add-on	● Optional Add-on
	Integration with Buyer AD/Directory for user aware policies. Up to 5 AD servers/domains	✕	✕	✓
	Firewall based traffic shaping for application prioritisation, including bandwidth limiting of applications Up to 3 traffic shaping profiles	✕	✕	● Optional Add-on

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN**

Public Sector



Professional Services

Supplier offers a range of professional services including technical consultancy, project management and on-site service management. The Charges associated with these services are as follows:.

Charges	
	Maximum daily rates excluding expenses
Consultants	
Junior Consultant	
Consultant	
Senior Consultant	
Principal Consultant	
Partner/ Director	
Contractors / IT Specialists	
Senior Analyst/ Team Leader	
Systems Analyst & Designers	
Analyst/ Programmers	
Application Programmers	
System Programmers	
Database Administrators	
Network Administrators	
Capacity Planners	
Configuration Managers	
IT Trainers	
Documentation Specialists	
Project Administrators	

10. Key Sub-Contractors

10.1. Openreach Limited

- a) Kelvin House, 123 Judd Street, London, United Kingdom, WC1H 9NP
- b) 10690039

10.2. Virgin Media Limited

- a) Media House, Bartley Wood Business Park, Hook, Hampshire, RG27 9UP
- b) 02591237

10.3. CityFibre Limited

- a) 15 Bedford Street, London, England, WC2E 9HE
- b) 09759465

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services**

Vodafone IP-VPN

Public Sector

**11. Definitions**

The following definitions are applicable to this Service Offer.

Access Method	the method of accessing the internet by Buyer, either via an Access Circuit or via Network Based Internet Access.
Acknowledgement	a confirmation given to Buyer that a particular request or Incident raised is valid and the provision to Buyer of a unique reference for it. "Acknowledge" shall be construed accordingly.
ADSL	asymmetric digital subscriber line.
Agreement	means the Call-Off Contract and Service Offer.
Asymmetric Access Bandwidths or Asymmetric	ADSL and/or VDSL access circuits.
AUP	Vodafone's acceptable use policy available on request.
Availability	the percentage of time the Service is available for use at the Service Demarcation Point of each Buyer Site in a Monthly Measurement Period.
Backbone	the IP Backbone Core and related infrastructure beyond the IP Backbone Core
BPE (Buyer Premises Equipment)	the edge router at a Buyer Site provided and managed by the Supplier (Fixed Equipment) where set out in the Call-Off contract.
Buyer Equipment	hardware, Software or any other tangible material not supplied by Vodafone that is used with or to access the Service. Any Equipment Buyer purchases from Vodafone shall be considered to be Buyer Equipment once title has passed to the Buyer.
Buyer Group	Buyer and any company in which Buyer has the beneficial ownership of more than 50% of the issued share capital, or the legal power to direct the general management of the company in question, either at or after the date of the Call-off Contract.
BMI	a "Buyer major incident", being the highest category of Impact for an Incident resulting in significant disruption to the business of Buyer.
Buyer's Service Desk	is the service desk provided by Buyer which will be the initial point of contact between Vodafone and Buyer.
Buyer Site	as the context permits a Buyer's premises (either owned by Buyer or a third party) which Vodafone needs to access in order to deliver or install Equipment and/or to provide the Services or the location where the Services are to be provided, as set out in the Call-Off Contract.
Buyer Supplied Router	the Buyer-edge router at a Buyer Site provided and managed by the Buyer where set out in the Call-Off contract.
	a document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a "forward schedule of change".
Class(es) of Service CoS	the classes of Service used to prioritise network traffic

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services**

Vodafone IP-VPN

Public Sector



Configuration Change	any Hard Configuration Change and/or any Soft Configuration Change.
Default CoS	the CoS allocated to any traffic not assigned to Standard CoS, Enhanced CoS or Premium CoS.
DSL	a Digital Subscriber Line
EA Country Group	the group of countries set out in the Extended Access Country Groups table.
EFM	Ethernet First Mile which is a copper-based Ethernet access technology which may be used to provide symmetric bandwidth access circuits of 512Kbps to 20Mbps.
End Of Life	where Vodafone or a manufacturer of Equipment declares that the type of Equipment is end-of-life (or otherwise stops marketing, selling or supporting it).
Enhanced CoS	a medium level of CoS consisting of three levels (1, 2 and 3) that prioritises traffic over classes of lower priority to reduce delayed or dropped traffic.
Equipment	hardware, Vodafone Software, and any other tangible equipment (other than SIMs) supplied by, or on behalf of, Vodafone to Buyer for use in receiving the Services. Equipment excludes Buyer Equipment.
Essential Outage	an Outage that is not a Planned Outage including, but not limited to, Outages caused by a force majeure event or an act or omission of any third party which is beyond Vodafone's reasonable control.
Excluded Event	any of the following: (a) fault or incident with any other Vodafone service purchased under a separate Service Offer under the framework; (b) a fault or incident in, or any other problem associated with, non-Vodafone supplied power, any Buyer Equipment, Buyer Supplied Router, non-maintained structured cabling, Buyer-contracted third party local internet access (in conjunction with Secure Internet Site Access), a Cloud Provider Data Centre as detailed in this Service Offer, or other systems or networks not operated or provided by Vodafone (including an Incident relating to consumption of services over the internet); (c) a fault or incident caused by Buyer's negligence, act or omission or that of any third-party not within Vodafone's direct control; (d) a fault, incident or delay that arises as a result of a request by the Buyer for an expedited delivery of the Service; (e) the Buyer not performing or a delay in performing any of the Buyer obligations or conditions of use set out in the Agreement; (f) the Buyer requesting Vodafone to modify a Buyer Site, or to test one, although no Incident has been detected or reported in accordance with the Agreement; (g) Service suspension or a Force Majeure event in accordance with the NSF framework; (h) the inability or refusal by a third-party supplier to provide input products at a Buyer Site where the Service uses these to deliver the access circuit; (i) a Configuration Change in the process of implementation; (j) an Planned Works; (k) any failure to achieve service degradation targets resulting from a rate adaptive ADSL, or VDSL2, line retrain or due to performance issues, such as noise or vibrations, impacting copper access technologies supporting asymmetric or symmetric access circuits; (l) any degradation of performance that is caused by, or for any fault or incident in, the access circuit that occurs as a result of, or in connection with, technical limitations beyond Vodafone's control; (m) Vodafone being unable to access or being delayed in accessing the Buyer Site (where a Buyer Site visit is required) due to reasons outside its control, including, inclement weather or Buyer's refusal to admit Vodafone; or (n) any other circumstances caused by events for which Vodafone is not liable in accordance with the terms of the Agreement.
Extended Access	an inter-provider MPLS interconnection that extends the Service using third party networks.

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services**

Vodafone IP-VPN

Public Sector



Extended Access Country Group	the group of countries set out in the Extended Access Country Group table.
Fixed Equipment	hardware, Vodafone Software, BPE and any other tangible equipment (other than SIMs and mobility equipment) supplied by or on behalf of, Vodafone to Buyer for use in receiving the Services.
GPON	Gigabit capable Passive Optical Network. An access technology which is used to provide Fibre to the Premises (FTTP). Access circuits using this access method offer contended bandwidth.
GSM Gateway	any equipment containing a SIM card which enables the routing of calls from fixed apparatus to mobile equipment by establishing a mobile-to-mobile call.
Hard Configuration Change	a change to the Service that may include one or more of the following: (a) transfer of the Service from one Buyer Site to another; (b) migrating between physical service access options (including port speed or port type); (c) modifications requested by Buyer to alter the Service at a Buyer Site requiring physical intervention; (d) physical movement of a Buyer Site; and/or (e) removing a Buyer Site from the Service.
Helpdesk(s)	the Buyer Services Helpdesk
	a measure of the effect of an incident, problem or change on business processes. impact is often based on how service levels will be affected. Impact and urgency are used to assign priority.
Incident	an unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected Service is also an Incident.
Incident Management	the end-to-end management of Incidents by Vodafone.
Incident Record	a record containing the details and lifecycle of an Incident.
Infrastructure Services	an IT service that is not directly used by Buyer's business but is required for the provision of other IT services (for example either a Functional Service, connectivity service, hosting service or any combination thereof).
Initial Response	a first response from Vodafone to an individual raising a request or Incident, such as answering the telephone or replying to an email.
IP Backbone Core	Vodafone's multi-protocol label switching (MPLS) enabled network platform.
Jitter	a measure of the variation between the arrival of consecutive 64-byte IP packets caused by network congestion, timing differences or route changes.
Monthly Measurement Period	the period from when the service commences up to the end of the calendar month and then each calendar month thereafter (save for the last month which will be the beginning of the calendar month up to the termination date or expiry of the Service).
Network	the communications network together with the equipment and premises that are connected to such network and which are used by Vodafone to perform the Services.
NTE	Equipment used to terminate a Buyer connection where Buyer has Ethernet access or a local internet access provider's device where Buyer has Secure Internet Site Access.
Planned Outage	the scheduled unavailability of an Infrastructure Service.

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services**

Vodafone IP-VPN

Public Sector



PoP	Point of presence.
PoP Tier	one of the groups of coverage set out on in the PoP Tiers & SISA Bands schedule
Premium CoS	the highest level of CoS, prioritised over all other traffic.
	a cause of one or more Incidents. The cause is not usually known at the time a problem record is created, and the problem management process is responsible for further investigation.
	a record containing the details and lifecycle of a Problem.
Resolution	the exercise by Vodafone of its reasonable endeavours to repair the root cause of an Incident or Problem, or to implement a workaround.
Round Trip Delay or RTD	the total time taken for an IP packet to pass from one Router to another Router and then back to the original Router
Router	a router which is Equipment used in connection with the Service.
Secure Internet Site Access or SIS	the provision of access to the Service using an encrypted tunnel over Vodafone provided local in country internet access or off-net access.
Services	the Vodafone product(s) detailed in this Service Offer.
Service Commencement Date	the date of completion of Vodafone's testing when the Service is ready for use.
Service Degradation	one or all of the following metrics: Jitter, Round Trip Delay and/or packet loss.
Service Demarcation Point	(a) the port between the Router and the Buyer Network for the Managed Service package; (b) the service interface of the access circuit for the Wires Only Service package; (c) the NTE where Ethernet technology is used for the Wires Only Service package; (d) the access interface on the Maintained Router for the Maintained Service package.
Service Request	a request from a user for information, or advice, or for a Standard Change or for access to an IT service made in accordance with the requirements of the relevant Service Request Catalogue.
Service Request Catalogue	the service request catalogue for IPVPN, as made available to Buyer and updated by Vodafone from time to time.
Severity Level(s)	a categorisation of the severity of an Incident as determined by Vodafone in Vodafone's discretion as set out in clause 1 of the Service Levels
SISA Band	one of the groups of coverage set out in the Coverage Bands table
SISA Gateway	the device used to terminate encrypted tunnels over the internet as part of the provision of Secure Internet Site Access
Site Classification	the classification assigned to a Buyer Site in accordance with the Site Classification Matrix (the matrix that defines the Site Classification depending on its topology and access technology set out in the Site Classification table.
Site Survey	a survey of a Buyer's Site to assess whether (in Vodafone's opinion) the existing infrastructure is sufficient for providing the Services and detailing what the Buyer needs to do to receive the Service.

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services**

Vodafone IP-VPN

Public Sector



Soft Configuration Change	a change to the Service provided to Buyer that is not a Hard Configuration Change or a Normal Change, including the following: (a) modification of the configuration of the Buyer's VPN, at Buyer's request, that is not classified as a Hard Configuration Change; and/or (b) modifying the bandwidth allocated to a CoS for a Buyer Site.
	a machine executable computer program, software module or software package or any part thereof (in object code only) which Vodafone licences to Buyer, or grants Buyer access to, as part of the Service, irrespective of how it is stored or executed, and including all fixes, modifications, enhancements, translations, updates, upgrades and derivative works.
Standard Change	a pre-approved Change that is low risk, relatively common and follows a procedure or work instruction. The types of Standard Changes available are listed in a Service Request Catalogue.
Standard CoS	a lower level of CoS consisting of one level that prioritises traffic over Default CoS to reduce delayed or dropped traffic.
Supplier	where used in this Service Offer or Call-Off Contract means Vodafone
Third Party Provider	a Key Subcontractor or third party contracted by Vodafone or Buyer that provides a Service, or that provides a service that connects to a Service.
Unavailable or Unavailability	a Buyer Site cannot exchange data with another Buyer Site for reasons other than an Excluded Event.
User	an individual end user of the Services who is approved by Buyer and who must be a permanent or temporary employee or sub-contractor of Buyer unless otherwise specified in this Agreement.
User Details	a username, password, or other access information used by a User to access the Service and/or Equipment.
VDSL2	an access method which uses Fibre to the Cabinet (FTTC) and very-high speed digital subscriber line 2 (VDSL2) technologies, and access circuits using this access method offer contended bandwidth.
Vodafone Software	any Software supplied by Vodafone or its licensors to Buyer (including Software embedded in any Equipment).
Vodafone Supplied Router	the Equipment which is a Buyer-edge router at a Buyer Site provided and managed by Vodafone.
VPN	Virtual private network
VRF	is a technology included in internet protocol network routers that allows multiple instances of a routing table to exist in a router and work simultaneously. This increases functionality by allowing network paths to be segmented without using multiple devices
Wires Only	the Service package where the Buyer supplies, installs, maintains and manages the Buyer Supplied Router.
Working Days	Monday to Friday inclusive, other than public holidays in the UK.
Working Hours	the hours between 8.00am and 6.00pm on each Working Day.

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services**

Vodafone IP-VPN

Public Sector

**Appendix 1 – Service Availability****1. Service Availability**

- 1.1. Calculation: Percentage Availability is calculated as: $[(A - B)/A] \times 100$. "A" equals the number of minutes in each full month e.g., during a 30-day monthly period A will equal 43200. "B" equals the number of whole minutes when the Service is Unavailable in the Monthly Measurement Period.
- 1.2. Service Levels: The following Availability Levels apply to each Buyer Site in a relevant PoP Tier, SISA Band or Extended Access Country Group depending on the Site Classification:
- a) Target Availability – PoP Tier 1 – PoP Tier 5

	Pop Tier 1		Pop Tier 2		Pop Tier 3		Pop Tier 4		Pop Tier 5	
Site Classification	% Service Availability	*Minutes Unavailable	%Service Availability	*Minutes Unavailable	%Service Availability	*Minutes Unavailable	%Service Availability	*Minutes Unavailable	%Service Availability	*Minutes Unavailable
Business Basic	96.50	1533	93	3066	93 (SLO)	3066	None	N/A	None	N/A
Business Standard	98	876	96	1752	96 (SLO)	1752	None	N/A	None	N/A
Corporate Basic	99.90	43.8	99.85	65.7	99.4	262.8	98 (SLO)	876	98.88	491
Corporate Standard	99.95	21.9	99.90	43.8	99.6	175.2	98.8 (SLO)	525.6	99.44	245*
Corporate Core	99.99	4.38	99.95	21.9	99.7	131.4	99 (SLO)	438	99.72	123
Corporate – Core Plus	99.995	2.19	99.99	4.38	N/A	N/A	N/A	N/A	N/A	N/A

*Only when secondary circuit over Ethernet, EFM or Leased Line. Unavailable minutes shown above are an example and assumes a 30-day monthly period.

- b) Target Availability – Secure Internet Site Access:

Site classification	Service availability	* Minutes Unavailable
SISA IPsec Only	99.99%	4.38 minutes
SISA Business Basic	93% (SLO)	3066 minutes
SISA Business Standard	93.5% (SLO)	3220 minutes
SISA Corporate Basic	98% (SLO)	876 minutes

*Unavailable minutes shown above is an example and assumes a 30-day monthly period.

- c) Target Availability – Extended Access:

EA Country Group	Single access Buyer Site	Dual access Buyer Site
1	99.7%	99.9%
2	99.2%	99.5%
3	99.0%	99.2%

2. Service Degradation

- 2.1. The Service Degradation Levels apply when: (a) Buyer Sites are: (i) directly connected to the IP Backbone Core at one of the available symmetric bandwidth options, or (ii) connected using the Asymmetric Bandwidth option if the target explicitly states it applies to an Asymmetric Service; (b) the distance between the Vodafone Managed Router (as applicable to the

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services****Vodafone IP-VPN****Public Sector**

Service Level or SLO) and the IP Backbone Core is less than 150 kilometres; (c) where symmetric bandwidth access circuits are provided, the minimum available port bandwidth, is at least 1.5Mbps; (d) the IP packet size is 64 bytes for Premium CoS and the average packet size for Standard and Enhanced CoS is 384 bytes; (e) Premium CoS bandwidth, as applicable, at the Buyer Site is a maximum of 50% of the port bandwidth; and (f) apply from the most recent commencement date for the relevant Buyer Site.

2.2. The Service Degradation Levels do not apply: (a) to Severity Level 1 or 2 Incidents; (b) where the Incident is due to an Excluded Event; and/or (c) to local internet access as part of Secure Internet Site Access service (if ordered by the Buyer as an Optional Service Element) and/or (c) if Buyer exceeds the bandwidth specified in the Call-Off Contract for the relevant Class of Service.

2.3. Service Degradation Measurements:

a) Round Trip Delay ("RTD"):

- i) The Round-Trip Delay SLO and Service Levels are measured as the total time taken for an IP packet to pass from one applicable Router to another applicable Router and then back to the original Router. The RTD SLO and Service Levels will be calculated as the average of all measurements taken in the Monthly Measurement Period.
- ii) The RTD Service Level Objectives for the IP Backbone Core between two IP Backbone Core Routers are set out below:

CoS	Service Level
	RTD IP Backbone Core (between two IP Backbone Core Routers)
Premium CoS	Section 1 of the Round-Trip Delay Table
Enhanced CoS	Section 1 of the Round-Trip Delay Table
Standard CoS	n/a
Default CoS	n/a

b) Packet Loss:

- i) Packet loss measures the percentage of IP packets that are not successfully sent over the IP Backbone Core during the Monthly Measurement Period.
- ii) The Service Levels for packet loss is as follows:

CoS	Service Level		
	Both Buyer Sites connected using Symmetric bandwidths	One or both Buyer Sites connected using Asymmetric bandwidths	Extended Access
Premium CoS	0.04%	0.2%	0.1%
Enhanced CoS	0.06%	0.3%	0.5%
Standard CoS	0.08%	n/a	n/a
Default CoS	n/a	n/a	n/a
*Assumes the use of 64-byte IP packets.			
**Assumes the use of 384-byte IP packets.			

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services**

Vodafone IP-VPN

Public Sector



c) Jitter

- i) Jitter measures the variation between the arrival of consecutive 64-byte IP packets caused by network congestion, timing differences or route changes as an average over the Monthly Measurement Period.
- ii) The jitter Service Levels below apply to pairs of Buyer Sites connected with Asymmetric or symmetric bandwidths.

CoS	Access Circuit bandwidth/ connection method:	Service Level	Service Level – Extended Access
Premium CoS only	<1 Mbps	67 milliseconds	20 milliseconds
	1 Mbps to 10 Mbps	20 milliseconds	
	>10 Mbps	<10 milliseconds	
	>155 Mbps	<5 milliseconds	

Each Buyer Site is classified into one of the following classes:

Site classification	Topology description	Applicable access technologies	
		Primary	Backup/Secondary
Business Basic	Single access.	ADSL / VDSL / GPON	N/A
Business Standard*	Single access with a back-up (active or passive). Single or dual Buyer Edge ("CE") routers (where advised). The backup is connected to a different Provider Edge ("PE") router than the primary service wherever possible.	ADSL / VDSL / GPON	ADSL / VDSL / GPON / SISA / VSAT
Corporate Basic	Single access. Optional secondary access to same PoP.	Ethernet	N/A
Corporate Standard	Single access with a backup (active or passive). Single or Dual CE router (where advised). The backup is connected to different PE router wherever possible.	Ethernet	ADSL / VDSL / GPON / SISA
Corporate Core	Dual CE routers; or Cloud Provider Demarcation Point (Cloud Connect). Dual Access/PoP. Dual building entry points.	Ethernet	Ethernet

RM6116 Network Services 3**Lot 1a – Inter site Connectivity/Data Access Services**

Vodafone IP-VPN

Public Sector



Site classification	Topology description	Applicable access technologies	
		Primary	Backup/Secondary
Corporate Core Plus (Only applies to PoP Tier 1&2)	Dual CE routers. Dual Access/PoP with 3 metre separation. Separate building entry points.	Ethernet	Ethernet
SISA IPsec Only	Gateway for termination of regional SISA IPsec traffic.	N/A	N/A
SISA Business Basic	Single access SISA.	SISA Broadband Access (ADSL, VDSL, FTTP)	N/A
SISA Business Standard	Single access SISA with IPsec Tunnels to separate SISA Gateways.	SISA Broadband Access (ADSL, VDSL, FTTP)	2nd IPsec tunnel to separate SISA Gateway
SISA Corporate Basic	Single access SISA connection.	SISA Dedicated Access (Ethernet,)	N/A

*Due to ongoing technical advances and the removal of copper access infrastructure by many network operators, DSL access may become unavailable for any given Buyer Site during the contract term. As a result, Business Standard topology will no longer be an option for that Buyer Site. Vodafone will discuss options with the Buyer if DSL technology becomes unavailable at any Buyer Site which may attract an additional charge and/or a reduction in availability SLA.

RM6116 Network Services 3

Lot 1a – Inter site Connectivity

Vodafone IP-VPN

Public Sector



PoP Tiers: The PoP tiers include the locations, service availability tier and incident resolution time tier in the table below:

PoP Country	PoP Location	Region	Service availability tier	Incident resolution tier
Angola	Luanda	Africa	5	5
Argentina	Buenos Aires	LATAM	2	2
Australia	Adelaide	APAC	1	1
Australia	Brisbane	APAC	1	1
Australia	Melbourne	APAC	1	1
Australia	Perth	APAC	1	1
Australia	Sydney	APAC	1	1
Austria	Vienna	Europe	1	1
Bahrain	Manama	Middle	3	3
Belgium	Brussels	Europe	1	1
Botswana	Gaborone	Africa	5	4
Brazil	Rio de Janeiro	LATAM	2	2
Brazil	Sao Paolo	LATAM	3	2
Bulgaria	Sofia	Europe	3	3
Cameroon	Douala	Africa	5	5
Canada	Montreal	US	1	1
Canada	Toronto	US	1	1
China	Beijing	APAC	1	1
China	Guangzhou	APAC	1	1
China	Shanghai	APAC	1	1
Cote D'Ivoire	Abidjan	Africa	5	5
Czech Republic	Prague	Europe	1	1
Denmark	Copenhagen	Europe	1	1
Djibouti	Djibouti	Africa	5	5
DRC	Kinshasa	Africa	5	4
DRC	Lubumbashi	Africa	5	4
Egypt	Cairo	Africa	3	3
Equatorial Guinea	Malabo	Africa	5	5
Ethiopia	Addis Ababa	Africa	5	5
Finland	Helsinki	Europe	1	1
France	Marseille	Europe	1	1
France	Paris	Europe	1	1
Germany	Dusseldorf	Europe	1	1
Germany	Frankfurt	Europe	1	1
Germany	Hamburg	Europe	1	1
Ghana	Accra	Africa	5	4
Greece	Athens	Europe	1	1
Hong Kong	Hong Kong	APAC	1	1
Hungary	Budapest	Europe	1	1
India	Bangalore	APAC	2	2
India	Chennai	APAC	2	2
India	Delhi	APAC	2	2
India	Mumbai	APAC	2	2
India	Pune	APAC	2	2
India	Gurgaon	APAC	3	1
India	Ahmadabad	APAC	3	1
India	Jaipur	APAC	3	1

PoP Country	PoP Location	Region	Service availability tier	Incident resolution tier
India	Vadodara	APAC	3	1
India	Thane	APAC	3	1
India	Noida	APAC	3	1
India	Chandigarh	APAC	3	1
India	Coimbatore	APAC	3	1
Indonesia	Jakarta	APAC	3	3
Ireland	Armagh	Europe	1	1
Ireland	Dublin	Europe	1	1
Ireland	Lisburn	Europe	1	1
Ireland	London Derry	Europe	1	1
Ireland	Omagh	Europe	1	1
Ireland	Portadown	Europe	1	1
Ireland	Strabane	Europe	1	1
Israel	Rosh Ha'AYin City	Europe	1	3
Italy	Milan	Europe	1	1
Japan	Osaka	APAC	1	1
Japan	Tokyo	APAC	1	1
Kenya	Mombasa	Africa	5	4
Kenya	Nairobi	Africa	5	4
Kuwait	Kuwait	Middle East	1	1
Liberia	Monrovia	Africa	5	5
Madagascar	Antananarivo	Africa	5	5
Malawi	Blantyre	Africa	5	5
Malaysia	Kuala Lumpur	APAC	2	2
Mauritius	Ebene	Africa	5	5
Mexico	Monterrey	Americas	3	2
Mexico	Mexico City	Americas	3	2
Morocco	Rabat	Africa	3	3
Mozambique	Maputo	Africa	5	5
Namibia	Windhoek	Africa	5	5
Netherlands	Amsterdam	Europe	1	1
New Zealand	Auckland	APAC	2	1
Nigeria	Lagos	Africa	5	5
Norway	Oslo	Europe	1	1
Oman	Wattayah	Middle East	4	4
Philippines	Manila	APAC	2	2
Poland	Warsaw	Europe	1	1
Portugal	Lisbon	Europe	1	1
Portugal	Porto	Europe	2	1
Russia	Moscow	Europe	2	2
Romania	Bucharest	Europe	3	3
Rwanda	Kigali	Africa	5	5
Senegal	Dakar	Africa	5	5
Sierra Leone	Freetown	Africa	5	5
Singapore	Singapore	APAC	1	1
South Africa	Johannesburg	Africa	5	2
South Korea	Seoul	APAC	1	1

PoP Country	PoP Location	Region	Service availability tier	Incident resolution tier
Spain	Barcelona	Europe	1	1
Spain	Madrid	Europe	1	1
Swaziland	Mbabane	Africa	5	5
Sweden	Stockholm	Europe	1	1
Switzerland	Zurich	Europe	1	1
Taiwan	Taipei	APAC	3	1
Tanzania	Dar Es Salaam	Africa	5	2
Thailand	Bangkok	APAC	2	2
Thailand	Nonthaburi	APAC	2	2
Turkey	Istanbul	Europe	2	2
UAE	Abu Dhabi	Middle	4	4
UAE	Dubai	Middle	4	4
Uganda	Kampala	Africa	5	4
Ukraine	Kiev	Europe	1	1
UK	Birmingham	Europe	1	1
UK	Bracknell	Europe	1	1
UK	Bristol	Europe	1	1
UK	Edinburgh	Europe	1	1
UK	Glasgow	Europe	1	1
UK	Leeds	Europe	1	1
UK	London	Europe	1	1
UK	Manchester	Europe	1	1
UK	Swindon	Europe	1	1
USA	Atlanta	US	1	1
USA	Boston	US	1	1
USA	Charlotte	US	1	1
USA	Chicago	US	1	1
USA	Dallas	US	1	1
USA	Denver	US	1	1
USA	El Segundo	US	1	1
USA	Houston	US	1	1
USA	Jacksonville	US	1	1
USA	Los Angeles	US	1	1
USA	Memphis	US	1	1
USA	Miami	US	1	1
USA	New York	US	1	1
USA	Phoenix	US	1	1
USA	Portland	US	1	1
USA	San Francisco	US	1	1
USA	San Jose	US	1	1
USA	Seattle	US	1	1
USA	Washington D.C	US	1	1
Vietnam	Hanoi	APAC	3	1
Vietnam	Ho Chi Minh city	APAC	3	1
Zambia	Lusaka	Africa	5	5

RM6116 Network Services 3**Lot 1a – Inter site Connectivity****Vodafone IP-VPN**

Public Sector



SISA Bands: For the purposes of the Agreement, the SISA Bands shall include the locations in the tables below:

A	Austria, Belgium, Bulgaria, Denmark, Finland, Germany, Hong Kong, Japan, Netherlands, Norway, Singapore, South Korea, Sweden, Switzerland, UK
B	Albania, Algeria, Andorra, Australia, Azerbaijan, Bahrain, Bosnia and Herzegovina, Cambodia, Cameroon, Canada, China, Costa Rica, Croatia, Czech Republic, Ecuador, Egypt, El Salvador, Estonia, France, Guatemala, Honduras, Hungary, Iceland, Ireland, Israel, Italy, Jordan, Kuwait, Latvia, Lebanon, Lithuania, Luxembourg, Macedonia, Malaysia, Malta, Moldova, Monaco, Morocco, Nicaragua, Oman, Panama, Portugal, Qatar, Romania, Russia, San Marino, Saudi Arabia, Serbia, Slovakia, Slovenia, Spain, Taiwan, Tunisia, Turkey, United Arab Emirates, US, US (Alaska), US (Hawaii), Venezuela, Vietnam.
C	Afghanistan, Angola, Anguilla, Antigua and Barbuda, Argentina, Armenia, Bahamas, Bangladesh, Barbados, Belarus, Bermuda, Bhutan, Botswana, Brunei, Darussalam, Burkina Faso, Burundi, Cape Verde, Cayman Islands, Chile, Colombia, Congo, Cyprus, Dominica, Ethiopia, Faroe Islands, Fiji, Gabon, Georgia, Ghana, Gibraltar, Greece, Grenada, Guadeloupe, Guam, Guernsey, Haiti, India, Indonesia, Iran, Iraq, Isle of Man, Ivory Coast, Jamaica, Jersey, Kazakhstan, Kenya, Kyrgyzstan, Laos, Libya, Liechtenstein, Macau, Madagascar, Malawi, Maldives, Mali, Martinique, Mongolia, Montenegro, Montserrat, Mozambique, Namibia, Netherlands Antilles (Aruba), Netherlands Antilles (Bonaire), Netherlands Antilles (Curacao), Netherlands Antilles (St. Maarten), New Zealand, Nigeria, Pakistan, Palestine, Peru, Philippines, Poland, Puerto Rico, Reunion, Rwanda, Senegal, Serbia (Kosovo), Seychelles, South Africa, Sri Lanka, Sudan, Syria, Tajikistan, Tanzania, Thailand, Uganda, Ukraine, Uruguay, Uzbekistan, Yemen.
D	American Samoa, Belize, Benin, Bolivia, Brazil, Central African Republic, Chad, Congo, Dem. Rep. (former Zaire), Cuba, Djibouti, Dominican Republic, East Timor, Equatorial Guinea, Eritrea, French Guiana, French Polynesia, Gambia, Guinea, Guinea-Bissau, Guyana, Liberia, Mauritania, Mauritius, Mexico, Myanmar, Nepal, New Caledonia, Niger, Northern Mariana Islands, Palau, Papua New Guinea, Paraguay, Saint Barthélemy, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Sierra Leone, Solomon Islands, South Sudan, Suriname, Swaziland, Togo, Trinidad and Tobago, Turks and Caicos Islands, Virgin Islands (British), Virgin Islands (U.S.), Zambia, Zimbabwe

RM6116 Network Services 3**Lot 1a – Inter site Connectivity****Vodafone IP-VPN****Public Sector**

Extended Access Group: 1		
Country	Region	Carrier
Jordan	Middle East	Batelco
Kuwait	Middle East	Batelco
Qatar	Middle East	Batelco
Saudi Arabia	Middle East	Batelco
Kuwait	Middle East	Bharti Airtel
Namibia	Africa	Bharti Airtel
China	Asia	China Telecom
China	Asia	China Unicom
China	Asia	CITIC Telecom CPC *
Taiwan	Asia	CITIC Telecom CPC
Cambodia	Asia	FPT
Laos	Asia	FPT
Myanmar	Asia	FPT
Vietnam	Asia	FPT
Argentina	Central & S America	Neutrona (IFX)
Bolivia	Central & S America	Neutrona (IFX)
Brazil	Central & S America	Neutrona (IFX)
Chile	Central & S America	Neutrona (IFX)
Colombia	Central & S America	Neutrona (IFX)
Ecuador	Central & S America	Neutrona (IFX)
Guatemala	Central & S America	Neutrona (IFX)
Mexico	Central & S America	Neutrona (IFX)
Paraguay	Central & S America	Neutrona (IFX)
Perú	Central & S America	Neutrona (IFX)
Venezuela	Central & S America	Neutrona (IFX)
Bangladesh	South Asia	PCCW
Botswana	Africa	PCCW
Cook Islands	Pacific	PCCW
Fiji	Pacific	PCCW
Ghana	Africa	PCCW
Kenya	Africa	PCCW
Kiribati	Pacific	PCCW
Mauritius	Africa	PCCW
Mozambique	Africa	PCCW
Namibia	Africa	PCCW
New Caledonia	Pacific	PCCW
Nigeria	Africa	PCCW
Niue	Pacific	PCCW
Norfolk	Pacific	PCCW
Pakistan	South Asia	PCCW
Papua New Guinea	Pacific	PCCW
Samoa	Pacific	PCCW
Solomon Island	Pacific	PCCW
South Africa	Africa	PCCW
Sri Lanka	South Asia	PCCW
Tanzania	Africa	PCCW
Tonga	Pacific	PCCW

RM6116 Network Services 3**Lot 1a – Inter site Connectivity**

Vodafone IP-VPN

Public Sector



Extended Access Group: 1		
Country	Region	Carrier
Uganda	Africa	PCCW
Vanuatu	Pacific	PCCW
Zambia	Africa	PCCW
Zimbabwe	Africa	PCCW
Japan	Asia	SoftBank Telecom
Argentina	Central & S America	Telecom Italia Sparkle (TIS)
Bolivia	Central & S America	Telecom Italia Sparkle (TIS)
Brazil	Central & S America	Telecom Italia Sparkle (TIS)
Chile	Central & S America	Telecom Italia Sparkle (TIS)
Colombia	Central & S America	Telecom Italia Sparkle (TIS)
Ecuador	Central & S America	Telecom Italia Sparkle (TIS)
Guatemala	Central & S America	Telecom Italia Sparkle (TIS)
Mexico	Central & S America	Telecom Italia Sparkle (TIS)
Paraguay	Central & S America	Telecom Italia Sparkle (TIS)
Perú	Central & S America	Telecom Italia Sparkle (TIS)
Venezuela	Central & S America	Telecom Italia Sparkle (TIS)
Italy	Europe	Telecom Italia Sparkle (TIS)
Greece	Europe	Telecom Italia Sparkle (TIS)
Malta	Europe	Telecom Italia Sparkle (TIS)
Malaysia	Asia	Telekom Malaysia
Canada	North America	Telus

*CITIC is available to existing CITIC Buyers only.

Extended Access Group: 2		
Country	Region	Carrier
Nigeria	Africa	Bharti Airtel
Saudi Arabia	Middle East	Bharti Airtel
South Africa	Africa	Bharti Airtel
Antigua	Caribbean	C&W Communications
Barbados	Caribbean	C&W Communications
Bermuda	North America	C&W Communications
British Virgin Islands	Caribbean	C&W Communications
Caribbean	North America	C&W Communications
Cayman Islands	Caribbean	C&W Communications
Dominica	Caribbean	C&W Communications
Grenada	Caribbean	C&W Communications
Jamaica	Caribbean	C&W Communications
St. Kitts	Caribbean	C&W Communications
St. Lucia	Caribbean	C&W Communications
St. Vincent	Caribbean	C&W Communications
Anguilla	Caribbean	C&W Communications
Montserrat	Caribbean	C&W Communications
Turks & Caicos	Caribbean	C&W Communications
Indonesia	Asia	TELIN Singapore
Argentina	Central & S America	TIWS
Bolivia	Central & S America	TIWS
Brazil	Central & S America	TIWS

RM6116 Network Services 3**Lot 1a – Inter site Connectivity**

Vodafone IP-VPN

Public Sector



Extended Access Group: 2		
Country	Region	Carrier
Chile	Central & S America	TIWS
Colombia	Central & S America	TIWS
Ecuador	Central & S America	TIWS
Guatemala	Central & S America	TIWS
Mexico	Central & S America	TIWS
Paraguay	Central & S America	TIWS
Perú	Central & S America	TIWS
Venezuela	Central & S America	TIWS
Angola	Africa	Vodacom Business Africa
Botswana	Africa	Vodacom Business Africa
Cameroon	Africa	Vodacom Business Africa
Cote D'Ivoire (Republic of)	Africa	Vodacom Business Africa
Djibouti	Africa	Vodacom Business Africa
DRC	Africa	Vodacom Business Africa
DRC	Africa	Vodacom Business Africa
Equatorial Guinea	Africa	Vodacom Business Africa
Ghana	Africa	Vodacom Business Africa
Kenya	Africa	Vodacom Business Africa
Kenya	Africa	Vodacom Business Africa
Lesotho	Africa	Vodacom Business Africa
Liberia	Africa	Vodacom Business Africa
Madagascar	Africa	Vodacom Business Africa
Malawi	Africa	Vodacom Business Africa
Mauritius	Africa	Vodacom Business Africa
Mozambique	Africa	Vodacom Business Africa
Namibia	Africa	Vodacom Business Africa
Nigeria	Africa	Vodacom Business Africa
Rwanda	Africa	Vodacom Business Africa
Senegal	Africa	Vodacom Business Africa
South Africa	Africa	Vodacom Business Africa
South Africa	Africa	Vodacom Business Africa
South Africa	Africa	Vodacom Business Africa
South Africa	Africa	Vodacom Business Africa
South Africa	Africa	Vodacom Business Africa
South Africa	Africa	Vodacom Business Africa
Swaziland	Africa	Vodacom Business Africa
Tanzania	Africa	Vodacom Business Africa
Tanzania	Africa	Vodacom Business Africa
Uganda	Africa	Vodacom Business Africa
Zambia	Africa	Vodacom Business Africa
Zimbabwe	Africa	Vodacom Business Africa
Cameroon	Africa	Vodacom Business Africa
Tanzania	Africa	Vodacom Business Africa
Ghana	Africa	Vodacom Business Africa
India	India	Vodafone India Limited (VIL)
Qatar	Middle East	Vodafone Qatar
Qatar	Middle East	Vodafone Qatar
Qatar	Middle East	Vodafone Qatar

RM6116 Network Services 3**Lot 1a – Inter site Connectivity**

Vodafone IP-VPN

Public Sector



Extended Access Group: 3		
Country	Region	Carrier
Angola	Africa	Internet Solutions
Ethiopia	Africa	Internet Solutions
Botswana	Africa	Internet Solutions
Ghana	Africa	Internet Solutions
Kenya	Africa	Internet Solutions
Mauritius	Africa	Internet Solutions
Mozambique	Africa	Internet Solutions
Namibia	Africa	Internet Solutions
Nigeria	Africa	Internet Solutions
South Africa	Africa	Internet Solutions
Tanzania	Africa	Internet Solutions
Uganda	Africa	Internet Solutions
Zambia	Africa	Internet Solutions
Zimbabwe	Africa	Internet Solutions
Guam	Pacific	PCCW
Nepal	South Asia	PCCW
Bangladesh	South Asia	TATA
Nepal	South Asia	TATA
Pakistan	MENA	TATA
Sri Lanka	South Asia	TATA
Kuwait	Middle East	Tawasul
Oman	Middle East	Tawasul
Qatar	Middle East	Tawasul
Saudi Arabia	Middle East	Tawasul
Algeria	Africa	Telecom Italia Sparkle (TIS)
Bosnia	Europe	Telecom Italia Sparkle (TIS)
Croatia	Europe	Telecom Italia Sparkle (TIS)
Cyprus	Europe	Telecom Italia Sparkle (TIS)
Egypt	Africa	Telecom Italia Sparkle (TIS)
KOSOVO	Europe	Telecom Italia Sparkle (TIS)
Libya	Africa	Telecom Italia Sparkle (TIS)
Montenegro	Europe	Telecom Italia Sparkle (TIS)
Morocco	Africa	Telecom Italia Sparkle (TIS)
Serbia	Europe	Telecom Italia Sparkle (TIS)
Slovenia	Europe	Telecom Italia Sparkle (TIS)
Tunisia	Africa	Telecom Italia Sparkle (TIS)
Indonesia	Asia	Telekom Malaysia
Sri Lanka	South Asia	Telekom Malaysia
Extended Access Group: Reasonable Endeavors		
Country	Region	Carrier
Tanzania	Africa	Bharti Airtel
UAE	Middle East	Bharti Airtel
Uganda	Africa	Bharti Airtel
Zambia	Africa	Bharti Airtel
Zimbabwe	Africa	Bharti Airtel
Algeria	Africa	Orange Business Services (France Telecom International)
Guinea	Africa	Orange Business Services (France Telecom International)
Mauritania	Africa	Orange Business Services (France Telecom International)
Ethiopia	Africa	PCCW
Egypt	Africa	Vodafone Egypt

RM6116 Network Services 3

Lot 1a – Inter site Connectivity

Vodafone IP-VPN

Public Sector



3. Section 1 – IP Backbone Core RTD Targets in Milliseconds (ms)

Round Trip Delay Service Level Targets between two IP Backbone Core Routers in milliseconds:
The Round Trip Delay Service Levels for the IP Backbone Core is calculated as the applicable IP Backbone Core RTD Target in the tables in Section 1 in this document x 1.2.

RM6116 Network Services 3

Lot 1a – Inter site Connectivity

Vodafone IP-VPN

Public Sector



Backbone Core RTD Targets in Milliseconds (ms) – Africa:

RTD Matrix	Angola	Botswana	Ivory Coast	Cameroon	Djibouti	DRC	Ghana	Equatorial Guinea	Kenya	Lesotho	Mauritius	Madagascar	Mozambique	South Africa	Malawi	Namibia	Nigeria	Senegal	Swaziland	Tanzania	Uganda	Zambia	Zimbabwe	UK
Angola		90	270	390	360	270	270	360	255	225	140	150	95	80	145	120	220	290	130	250	270	110	90	170
Botswana			310	380	190	130	300	400	90	40	70	85	40	20	100	60	120	330	80	75	105	55	45	210
Ivory Coast				280	390	310	220	300	305	315	350	365	330	300	350	325	220	230	370	280	300	340	320	110
Cameroon					460	390	130	370	375	385	410	410	380	370	420	395	150	300	420	340	390	390	380	180
Djibouti						380	390	510	115	190	230	255	160	175	230	225	335	440	230	120	130	215	195	325
DRC							325	410	280	140	160	170	125	125	220	155	315	340	160	340	310	170	145	220
Ghana								310	240	230	270	280	245	125	270	260	30	240	265	290	255	155	235	115
Equatorial Guinea									400	410	450	460	440	400	450	420	310	325	450	395	415	430	410	200
Kenya										90	130	135	60	75	170	125	230	335	125	30	30	120	100	220
Lesotho											70	80	45	30	110	65	120	335	105	75	110	60	45	210
Mauritius												120	75	55	140	95	150	375	120	115	145	95	70	250
Madagascar													130	95	155	160	210	440	180	150	175	145	105	260
Mozambique														40	95	70	125	370	80	65	80	60	45	270
South Africa															70	55	105	320	50	65	95	50	30	195
Malawi																115	200	405	155	135	165	105	90	275
Namibia																	130	345	120	120	140	85	60	220
Nigeria																		240	150	280	270	140	120	115
Senegal																			380	325	340	350	340	130
Swaziland																				120	175	90	105	270
Tanzania																					45	105	80	200
Uganda																						130	115	225
Zambia																							60	240
Zimbabwe																								215
UK																								

RM6116 Network Services 3

Lot 1a – Inter site Connectivity

Vodafone IP-VPN

Public Sector



IP Backbone Core RTD Targets in Milliseconds (ms) – UK:

Row Labels	UK - Aberdeen	UK - Addlestone	UK - Bedford	UK - Birmingham	UK - Bracknell	UK - Brighton	UK - Bristol	UK - Edinburgh	UK - Glasgow	UK - Inverness	UK - Leeds	UK - Livingston	UK - London	UK - Manchester	UK - Milton Keynes	UK - Newcastle	UK - Sheffield	UK - Swindon	UK - Tingley	UK - Warrington	UK - Watford
UK - Aberdeen	3	24	20	18	24	23	29	7	22	14	28	10	23	16	24	18	17	19	16	15	19
UK - Addlestone	24		16	10	13	16	16	19	23	22	14	18	15	13	20	16	13	12	13	12	
UK - Bedford	20	16		10	8	6	14	11	20	18	20	12	8	9	7	9	8	7	8	8	3
UK - Birmingham	18	10	10	4	7	10	10	12	20	16	14	12	8	6	15	9	7	6	6	6	8
UK - Bracknell	24	13	8	7	3	7	10	16	17	22	17	17	5	13	12	15	13	4	10	11	5
UK - Brighton	23	16	6	10	7		13	15	17	22	20	18	7	12	11	13	12	7	9	11	4
UK - Bristol	29	16	14	10	10	13	10	20	23	24	20	20	11	17	18	17	16	9	14	18	9
UK - Edinburgh	7	19	11	12	16	15	20		13	9	18	3	17	10	16	10	8	14	7	10	11
UK - Glasgow	22	23	20	20	17	17	23	13	16	20	27	17	18	11	23	14	13	17	11	10	14
UK - Inverness	14	22	18	16	22	22	24	9	20		26	9	21	14	22	16	15	17	14	14	18
UK - Leeds	28	14	20	14	17	20	20	18	27	26	18	22	18	17	24	19	17	16	16	16	7
UK - Livingston	10	18	12	12	17	18	20	3	17	9	22		17	10	16	10	9	13	10	10	14
UK - London	23	15	8	8	5	7	11	17	18	21	18	17	6	11	11	14	13	6	11	11	3
UK - Manchester	16	13	9	6	13	12	17	10	11	14	17	10	11	3	13	7	6	8	4	4	8
UK - Milton Keynes	24	20	7	15	12	11	18	16	23	22	24	16	11	13		14	12	11	12	13	7
UK - Newcastle	18	16	9	9	15	13	17	10	14	16	19	10	14	7	14		6	11	6	7	9
UK - Sheffield	17	13	8	7	13	12	16	8	13	15	17	9	13	6	12	6		9	3	5	7
UK - Swindon	19	12	7	6	4	7	9	14	17	17	16	13	6	8	11	11	9		8	7	5
UK - Tingley	16	13	8	6	10	9	14	7	11	14	16	10	11	4	12	6	3	8		4	6
UK - Warrington	15	12	8	6	11	11	18	10	10	14	16	10	11	4	13	7	5	7	4		7
UK - Watford	19		3	8	5	4	9	11	14	18	7	14	3	8	7	9	7	5	6	7	

RM6116 Network Services 3

Lot 1a – Inter site Connectivity

Vodafone IP-VPN

Public Sector



Section 2 – Round Trip Delay Service Level Targets – Extended Access

The following targets are indicative only.

Round Trip Delays in Milliseconds (ms) for Cable & Wireless Communications (Caribbean):

	Antigua	Barbados	BVI	Cayman	Dominica	Grenada	Jamaica	St. Kitts	St. Lucia	Miami NNI	NY NNI
Antigua		8	5	52	3	12	59	8	5	28	58
Barbados	13		13	60	8	17	68	17	3	36	66
BVI	5	13		47	8	17	53	4	10	23	53
Cayman	52	60	47		55	64	54	50	57	23	53
Dominica	3	11	8	55		9	8	11	7	31	61
Grenada	12	20	17	64	9		63	20	8	40	70
Jamaica	58	68	53	8	63	70		57	63	30	60
St. Kitts	8	17	3	50	11	20	57		13	27	56
St. Lucia	5	13	10	57	8	7	63	13		33	63
Miami NNI	28	37	24	24	32	41	32	28	33		30
NY NNI	59	65	53	54	62	71	63	56	63	30	

Round Trip Delays in Milliseconds (ms) for Telefonica (Latin America):

	Bogota	Buenos Aries	Lima	Miami NNI	Mexico	Sao Paulo	Chile	London NNI
Bogota		265	184	108	166	264	237	270
Buenos Aries	265		110	187	261	50	57	332
Lima	184	110		101	171	165	59	249
Miami NNI	108	187	101		73	163	144	59
Mexico	166	261	171	73		237	333	188
Sao Paulo	264	50	165	163	237		105	308
Chile	237	57	59	144	333	105		297
London NNI	270	332	249	59	188	308	297	

Round Trip Delay in Milliseconds (ms) for China Telecom (China):

	East China	Central China	West China
East China	120	200	320
Central China	200	200	320
West China	320	320	320

RM6116 Network Services 3

Lot 1a – Inter site Connectivity

Vodafone IP-VPN

Public Sector



Round Trip Delay in Milliseconds (ms) for Telekom (Malaysia):

	Malaysia	Singapore	Indonesia	Hong Kong	Egypt	Bahrain	London	New York	Los Angeles	Sri Lanka
Malaysia		25	40	60	170	170	250	310	250	85
Singapore	25		50	80	180	180	250	310	250	95
Indonesia	40	50		90	200	200	270	340	280	105
Hong Kong	60	80	90		230	230	300	370	270	130
Egypt	170	180	200	230		180	410	480	380	250
Bahrain	170	180	200	230	180		410	480	380	250
London	250	250	270	300	410	410		90	170	300
New York	310	310	340	370	480	480	90		90	370
Los Angeles	250	250	280	270	380	380	170	90		270
Sri Lanka	85	95	105	130	250	250	300	370	270	

Round Trip Delay in Milliseconds (ms) for Batelco (Middle East):

Region	Real time	Mission critical	Standard data
Gulf region	<=35 ms	<=40 ms	<=50 ms
Middle East region	<=45 ms	<=50 ms	<=55 ms

Round Trip Delay in Milliseconds (ms) for other carriers:

Carrier	Countries	Round Trip Delay
Telecom Italia Sparkle (Italy)	Italy	60 ms
Softbank Telecom (Japan)	Intra-Japan	35 ms
Telus (Canada)	Intra-Canada:	70 ms
	Canada-NY & LA NNIs	120ms
Tawasul (Middle East)	Between Kuwait; Oman; Qatar; & Saudi Arabia	60ms

Vodafone will make available to the Buyer Extended Access RTD Service Levels for countries not listed in this document upon request.

Network Based Internet Access, Secure Network Gateway and Secure Remote User Access Availability

Calculation: Percentage Availability is calculated as: [(A – B)/A] x 100.

“A” equals the number of whole minutes in the Monthly Measurement Period.

“B” equals the number of whole minutes that the Service is Unavailable in the Monthly Measurement Period

“Unavailable” or “Unavailability” means data cannot be transported through the applicable Service Demarcation Point for Enhanced NBIA, SRUA, and/or SNG Services for reasons other than Excluded Events.

a) Target Availability

	Single PoP location	Geographic Diversity
Percentage availability	99.9%	99.99%



vodafone
business

Together we can

RM6116 - Network Services 3

Service Offer Reference: RM6116-Lot1a-VodafoneLtd-#065

Lot(s): 1a

Effective Date: 12/06/2025

Expiry Date: 20/07/2027



Together we can
vodafone
business

RM6116 Network Services 2

Lot 1a – Inter site Connectivity / Data Access Services

Vodafone Dedicated Internet Access
Public Sector



Contents

1.	The Service – Overview and why Vodafone	3
2.	Conditions on the Buyer	3
3.	Outline Implementation Plan	9
4.	Exit Management Plan	9
5.	Service Level Agreement	10
6.	Optional Schedules	15
7.	Mandatory Schedules	15
8.	Service Description and Price Card	16
9.	Key Sub-Contractors	21
10.	Definitions	22
<hr/>		
	Annex 1 – Dedicated Internet Access Availability	27

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector****1. The Service – Overview and why Vodafone**

- 1.1. Dedicated Internet Access provides fast and reliable access to the Internet over a dedicated access circuit provided at a range of fixed and burstable bandwidths from 10Mbps to 10Gbps.
- 1.2. Vodafone will provide you with wide area connectivity for the provision of a managed or unmanaged point-to-point data-only connection and/or wide area connectivity for the provision of a managed or unmanaged point-to-internet/cloud data-only connection (the “Service”).
- 1.3. Vodafone is committed to providing our Buyers with a truly fast, reliable, and exceptional service. With Dedicated Internet Access from Vodafone, businesses that have outgrown or have greater demands that cannot be accommodated can benefit from our comprehensive portfolio of Connect, Communicate and Collaborate services. We can help businesses consolidate communications, simplify supplier management, and provide tangible cost savings. Vodafone’s strong relationship with the IP backbone allows us to be one of the world’s most reliable networks, making it simple to tailor Dedicated Internet Access to exactly the way you want it.

2. Conditions on the Buyer

- 2.1. In the event of a conflict between the terms and conditions included within this Service Offer and the RM6116 Framework or Call-Off terms, then the Framework or Call-Off terms will take precedence.

This Service Offer is available to Buyers that meet and agree to the following criteria:

- 2.2. General Conditions on the Buyer
 - a) **Authorised Users:** Access by Buyer to the Services and Equipment is limited to authorised Users. If Vodafone provides each authorised User with User Details, Buyer is responsible for: (a) The security of the User Details; and (b) providing Vodafone with the identity of the authorised Users and keeping that information current. Vodafone accepts no liability for any unauthorised or improper use or disclosure of any User Details. Buyer is liable for all acts and omissions conducted using the User Details up until the time that it informs Vodafone that they are being used without authority or may be compromised.
 - b) **Additional Service Recipient:** If Buyer wishes to add Additional Service Recipients, the Buyer shall: (a) provide the full corporate details of the Additional Service Recipient; (b) seek approval in writing from Vodafone; (c) inform the Additional Service Recipient of the contractual arrangements; and (d) agree to pay such additional charges as Vodafone may reasonably request in relation to the approval of such requests.
 - c) Save as expressly permitted under this Agreement, Buyer shall not resell, distribute, provide or sub-license the Services or Equipment (except Buyer Equipment) to any third party.
 - d) Buyer shall take appropriate measures to back up data and otherwise protect against loss of data under this Agreement.
 - e) **Terms of use:** Buyer shall not (a) make unauthorised modifications to the Services (b) use the Services as a means to establish permanent services, relay connections or interconnection services or any similar commercial activities, (c) do anything that causes the Network to be impaired; (d) use automated means to make calls, texts or send data (including via a GSM Gateway), unless expressly authorised in this Agreement or (e) use the Services in a way that may reasonably be considered to be a nuisance, defamatory, offensive, abusive, obscene or in a violation of any person’s rights or is illegal, fraudulent or contrary to good faith commercial practise to Vodafone’s detriment. Buyer shall comply with the AUP in using the Services. Buyer shall notify Vodafone immediately of any breach of security or unauthorised use of the Services.
 - f) **Service Monitoring:** Buyer gives express consent for Vodafone to monitor Buyer’s use of the service (and disclose and otherwise use the information obtained) only to: (a) the extent allowed by applicable law; (b) comply with applicable law; (c) protect the Network from misuse; (d) protect the integrity of the public internet and/or Vodafone’s systems and Networks; (e) the extent necessary to determine if Buyer has breached any conditions or restrictions on use of the Service; (f) provide the Service; and /or (g) take other actions agreed or requested by Buyer.

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector**

- g) Security: Buyer shall take reasonable steps in line with commercial good practise with entities it controls to limit misuse or threat to the Service or Network; and address any misuse or threat identified by Vodafone through the implementation of appropriate security or user controls. Buyer must seek prior approval from Vodafone before running any security tests, vulnerability scans or penetration tests on Equipment or Services.
- h) Buyer acknowledges that Buyer Equipment not authorised for use on the Network or any unauthorised attempt to repair or tamper with the Equipment may result in an impaired User experience and/or invalidate the manufacturer's warranty.
- i) Buyer must maintain, install, update, or follow Vodafone's reasonable recommendations regarding Equipment maintenance or upgrades.
- j) Equipment that is (i) out of manufacturer's warranty; or (ii) End Of Life is used at the Buyer's risk unless expressly agreed otherwise by Vodafone.
- k) Buyer shall:
 - i) Appropriately configure its Equipment to enable consumption of the Service.
 - ii) Maintain Buyers Equipment
 - iii) Provide details to facilitate the delivery, provisioning and billing of the Services requested by Vodafone at the time of ordering.
 - iv) Secure and keep in place or assist Vodafone to obtain (at the Buyer's cost), all relevant third party consents and approvals necessary for the purposes of providing, and preparing for the provision of, the Service. Such consents and approvals include obtaining any necessary wayleave on Vodafone's standard terms.
- l) Where Buyer terminates the Call-Off Contract during the Initial Period, the Buyer agrees to pay Vodafone's reasonable and proven losses resulting from the termination of the Call-Off Contract.
- m) Survey: This Service Offer and each Service Element is subject to survey. In the event a Site Survey output results in an increased price from the Call-Off Contract, the Buyer has the right to cancel the affected Service Element only in accordance with the terms of this Service Offer and Call-Off Contract.
- n) Unless otherwise agreed and stated in the Buyer's Call-Off Contract, the Buyer will be liable for any additional costs charged to Vodafone by third parties in connection with the provision of the Services. Such charges (often referred to as Excess Construction Charges) are detailed in the Ancillary Services section of this Service Offer. These charges will be notified to the Buyer before any construction works take place and In the event that this results in an increased price from the call off the Buyer has the right to cancel the affect Service Element only in accordance with the terms of this Service Offer and Call off Contract.
- o) Format: If Buyer requires this Service Offer (including bills, communications, or any document referred to therein) in a different format, please contact your Vodafone account manager, or frameworks_team@vodafone.com who will clarify Buyer requirements.

2.3. Fixed Services Conditions on the Buyer

- a) Service Commencement Date: Buyer shall notify Vodafone within 5 Working Days of the Service Commencement Date if the Services do not conform to the standard testing criteria and provide sufficient supporting details. Upon receipt of notification, Vodafone shall take reasonable action to meet the standard testing criteria.
- b) Vodafone-Owned Equipment: The following will apply where Vodafone provides Fixed Equipment for Buyer's use with a Service:

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector**

- i) Title: Title to the Fixed Equipment at all times belongs to Vodafone, its suppliers, or subcontractors (subject only to any rights which may be granted to Buyer in respect of Vodafone Software as set out in this Service Offer).
- c) Buyer Obligations: Buyer agrees to:
 - i) provide secure storage for Fixed Equipment that is sent to Buyer Sites prior to installation;
 - ii) use the Fixed Equipment only for the purpose of using the Services, in accordance with Vodafone's instructions and applicable Law;
 - iii) allow only Vodafone's authorised representatives to add to, move, modify, inspect, test or alter the Fixed Equipment (either on Buyer Site or remotely);
 - iv) adequately insure for, and notify Vodafone immediately of, loss, breach or suspected breach or damage to the Fixed Equipment;
 - v) only connect the Fixed Equipment to the Network using a network termination point that has been approved in advance by Vodafone;
 - vi) provide Vodafone with adequate power supply, connection, and space for the operation of the Fixed Equipment at Buyer Sites and in the case of BPE, patch cords and cabling and provide Vodafone 10 Working Days' notice of any known disruptive event (such as power disconnection); and additionally, specifically in relation to BPE:
 - A) appoint a local security representative to ensure the physical security of the BPE who will grant access by approved authorised personnel only and conduct routine physical checks, including ensuring tamper evident labels remain intact; and
 - B) ensure that the physical environment in which the BPE is housed is appropriate for the protective marking of the data being transmitted through such Fixed Equipment. In particular (i) BPE must be located in a communications room or other isolated area that is suitable to limit the occurrence of accidental or malicious damage to the BPE; and (ii) if the BPE is located in a shared environment, then it must be kept in a dedicated locked cabinet or rack. If that is not possible, robust access control mechanisms must be implemented by Buyer, with access only available with prior approval from Buyer's local security representative.
- d) Buyer Equipment: Where Buyer provides Buyer Equipment for use with a Service Buyer shall (and Buyer acknowledges that failure to do so will excuse Vodafone from liability for failure to deliver the Service):
 - i) install and configure the Buyer Equipment at the Buyer Sites by the date necessary to allow Vodafone to perform its obligations;
 - ii) maintain the Buyer Equipment including prompt installation of security patches and updates;
 - iii) promptly after the Service terminates, give Vodafone access to and reasonable help with disconnecting Buyer Equipment from the Service; and
 - iv) warrant and undertake that Buyer has full authority to permit Vodafone to perform the Services using the Buyer Equipment
- e) Buyer Sites: For the purposes of preparing for and delivery of the Services, Buyer shall:
 - i) carry out, or permit Vodafone or its subcontractors to conduct, a Site Survey;
 - ii) prepare the Buyer Site for the Services in accordance with Vodafone's instructions;
 - iii) allow and/or have in place (or assist Vodafone to do so at Buyer's cost) all third-party consents necessary to allow Vodafone or its subcontractors and agents (and obtain consents from third parties to allow) to:

RM6116 Network Services 2

Lot 1a – Inter site Connectivity / Data Access Services

Vodafone Dedicated Internet Access

Public Sector



- A) access the Buyer Sites, and any Buyer Equipment, Fixed Equipment or Equipment, and third-party property located there, as Vodafone reasonably requires to perform its obligations under this Agreement (including for the purposes of installing and uninstalling Equipment (whether in the Buyer Sites or outside) and providing and preparing for the provision of, the Services) and including access outside Working Hours; and
 - B) ensure that Buyer Sites are safe and have a suitable working environment.
 - f) Emergency Services:
 - i) General: In the event of a power cut or failure affecting Buyer's fixed line and/or broadband Service, or a failure of the internet connection on which the Service relies, Buyer may not be able to make calls including calls to emergency services. This may also affect any calls using the internet including calls to emergency services (see, below in 2.3(e)(iii)).
 - ii) Buyer obligations: Buyer shall:
 - A) provide Vodafone with complete and accurate Buyer Site address information; and
 - B) give Vodafone at least 30 days' written notice of any change to the location of any Fixed Equipment and to any change to the relevant Buyer Site address information
 - C) Buyer acknowledges that any failure to provide the information required may render emergency services unable to identify User's location.
 - iii) Calls using the internet: Additionally, where a Service places calls using the internet, Buyer shall:
 - A) make Users accessing the Service via a soft client aware that Vodafone may be unable to automatically determine their location if they make an emergency services call using the Services; and
 - B) ensure that such Users provide their location details in the event that they make an emergency services call using the Services. In the event of a power failure, the emergency call placed will be routed over the Network and not through the Service; and
 - C) provide registered address where a Buy or User will make calls over the internet including if there are multiple addresses where such calls will be made, and keep information on all such locations up to date.
- 24. Tiered Support Services conditions on Buyer
 - a) Buyer shall provide Vodafone with an email address for correspondence and shall be responsible for keeping Vodafone updated of any change.
 - b) Buyer shall carry out an initial analysis of any Incident reported to its Buyer's Service Desk, to establish whether the Incident should be referred to Vodafone. Buyer shall ensure it provides Vodafone with a key site list of all Buyer Sites that require BMI on or before the Service Commencement Date and shall further ensure that it notifies Vodafone of any updates or amendments to the key site list during the relevant Initial Period. The Buyer is required to ensure that the first key site list and any updates or amendments to the key site list are notified by email to the appointed service manager at Vodafone.
 - c) Service Desk: Buyer's Service Desk is the service desk provided by Buyer that will be the initial point of contact between Vodafone and Buyer, in relation to the Tiered Support Services.
 - d) Buyer shall nominate, and notify Vodafone of, one or more points of contact that shall be the primary management interface between Buyer and Vodafone and who shall have the authority contractually to bind Buyer for the purpose of enabling Vodafone to deliver the Tiered Support Services.

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector****2.5. Dedicated Internet Access Conditions on the Buyer**

- a) If using an existing Global IP-MPLS Network Access Bearer (i.e. Multi-Service Access Bearer - MSAB) for Dedicated Internet Access then Only Bandwidth and Router (if required) pricing should be applied.
- b) The Buyer shall provide 100/1000 Mbps Ethernet (IEE802.3-2015) LAN port and RJ45 cable, or for 10Gbps Ethernet (IEEE802.3-2015) services, 10GBASE-SR multi-mode fibre interface with LC connector to connect to the Supplier Network Termination Unit or where supplied the BPE router. Alternative interfaces can be agreed at time of order

The Buyer shall, at the time of ordering any of the Services under this Service Offer:

- c) Provide full details of the Services required and the Buyer site locations to enable validation of the Order Form. Such details shall include:
 - i) Access and/or Service Bandwidth required
 - ii) Rack location
 - iii) Room name or room number
 - iv) Building name, number, and floor.
 - v) Street name, town, city & postcode
- d) For each Buyer Site location, the Buyer shall provide a site contact name and contact details to include:
 - i) Contact telephone and email address
- e) Where the services are to be provisioned at a Buyer site that is owned by a third party landlord the Buyer shall advise the landlord or site owner's details including:
 - i) Landlord or site owner company name
 - ii) Name of nominated representative, including contact details
 - iii) Landlord or site owner building address including:
 - A) Room name and/or room number
 - B) Building name, number, and floor.
 - C) Street name, town, city & postcode
- f) The Buyer shall provide full details to enable billing of the Service including:
 - i) Billing contact name, telephone, and email contact details
 - ii) Purchase order references
 - iii) Billing entity/company name
 - iv) Billing address
 - v) VAT Registration Number
- g) Provide details to facilitate the delivery, provisioning and billing of the services requested by Vodafone at the time of ordering
- h) PSTN connection: Buyer shall not (and shall ensure that its Users shall not) connect or seek to connect the Services to the public switched telecommunications network (PSTN) where prohibited by Applicable Law (for example, in Turkey, Egypt and the UAE).

RM6116 Network Services 2

Lot 1a – Inter site Connectivity / Data Access Services

Vodafone Dedicated Internet Access

Public Sector



- i) Third-Party Provider: Where required by Applicable Law, the Service may be provided in a given country by a Third-Party Provider. Buyer shall be aware that in certain geographic locations, Vodafone will provide the Services through the use of a local Third-Party Provider ("Third-Party Provider Supplied Internet Access Services").
- j) Regulated Items: The export and/or import of certain Vodafone provided hardware and software (including, without limitation, the NTE if provided with Ethernet access, and any Managed Vodafone Supplied Router where contracted for) ("Regulated Items") is subject to domestic and/or foreign government export and/or import laws, rules, policies, procedures, restrictions and regulations ("Export/Import Controls"). Buyer represents and warrants the following for Regulated Items: (a) Buyer will export, import and/or disclose them only in strict compliance with applicable Export/Import Controls; and (b) Buyer will not try in any manner to evade US or any other jurisdiction's export controls on encryption. Buyer acknowledges that the Export/Import Controls may include a complete prohibition on the export, re-export, import and/or use of a Regulated Item in certain jurisdictions thereby precluding the use of Internet Access Services in these jurisdictions.
- k) Access Circuits: Vodafone will not be liable for any degradation of performance by, or fault to, the Access Circuit that occurs as a result of, or in connection with, technical limitations beyond Vodafone's control.
- l) DNS: Notwithstanding the assistance provided by Vodafone regarding DNS services as set out in the Service Specification, Buyer is responsible for ensuring that Buyer has all necessary rights or licences to use Buyer Domain Names or that Buyer have all necessary rights and consents to have them registered. .gov.uk Buyer Domain Names have additional terms provided by UK Government, Central and Digital Data Office which Buyer must comply with. The terms, as may be updated from time to time, are detailed at the following link www.gov.uk/guidance/additional-terms-for-govuk-agreements.
- m) IP Address and Autonomous System Numbers ("ASNs"): IP Addresses and ASNs that Vodafone make available for Buyer are not owned by Vodafone and they are subject to availability and to recall and suspension by the relevant authorising bodies.
- n) Black holing: Vodafone will Black Hole traffic to affected Services in response to a DDoS attack if (a) there is an attack on the Vodafone IP Backbone that is affecting the Service at one or more Buyer Sites; (b) Vodafone believes that there is a reasonable danger of congestion on a Service Element; and (c) if Buyer requests Vodafone to Black Hole specific IP Addresses or an IP Address range belonging to Buyer's network. Buyer may request to control the activation of Black Holing using the Service Change Request Procedure. Black Holed data will be lost and is not recoverable either during or following an occurrence of a DOS or DDoS attack. Vodafone is not responsible for any loss of data, loss of use or other loss arising from Black Holing.
- o) Providing Service over Existing Global IP-MPLS Network Access Bearers: Buyer may use an existing Global IP-MPLS Network Access Bearer (also referred to as existing MSAB (Multi-Service Access Bearer) within the Service Specification) for its IP-VPN Service also for Dedicated Internet Access. In this case, if Buyer terminates the IP-VPN Service at the Buyer Site, then the associated Dedicated Internet Access Service at that Buyer Site will also terminate.
- p) Any Changes to the Service, including ordering additional Services or amending an existing Service, shall be subject to the following service change request procedure ("Service Change Request Procedure"):
 - i) If either Party wishes to propose a change, it shall notify the other Party of that fact by sending a written request to the other Party's account manager, specifying in as much detail as is reasonably practicable the nature of the requested change.
 - ii) As soon as reasonably practicable after sending or receiving a written request for a change, Vodafone shall provide Buyer with a brief written proposal in relation to the relevant change (a "Change Control Proposal") including, where applicable, the following information: (i) details of the proposed change and its impact on the Service including, without limitation, any changes to the Service, Service Levels and any other variations to this Agreement; (ii) a statement of the cost and expense of implementation and

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector**

on-going operation of the relevant change, including any alteration of the charges or additional charges relating to the proposed change; (iii) a timetable for the implementation of the change; and (iv) details of the impact, if any, of the proposed change on any existing Services.

- iii) Buyer shall review Vodafone's Change Control Proposal as soon as reasonably practicable and will either accept or reject the proposed Change Control Proposal. If the Parties agree with the proposed Change Control Proposal, they shall issue an amendment to the Agreement authorising the change in the form of a change Order.
- iv) If it is necessary to use additional resources or to incur any other additional costs in making a change, they shall be calculated as a change to the Charges. Vodafone shall have no obligation to commence work in connection with any change until a relevant change Order authorising a change is executed by the Parties in writing.
- q) Where a new Buyer Site is added via the Service Change Request Procedure or where a Configuration Change to an existing Buyer Site has been approved via the Service Change Request Procedure, Vodafone will notify Buyer of specific site requirements at the Buyer Sites.

3. Outline Implementation Plan

- 3.1. Vodafone provides you with a comprehensive service, moving you from the Service Commencement Date per the Call-Off Contract to your first bill. Vodafone's outline Implementation Plan is detailed below, and this will be updated to become the draft Implementation Plan once the Call-Off Contract has been received by Vodafone:
- a) Vodafone will validate the Call-Off Contract containing the details of the Services being implemented under this Service Offer.
 - b) Vodafone will confirm the Call-Off Contract with a representative from the Buyer's organisation advising of any missing details.
 - c) Once all details are provided by the Buyer, Vodafone will submit the order for delivery and advise the Ready for Service target date to the Buyer.
 - d) Vodafone will manage the intermediate activities supporting the implementation process.
 - e) Vodafone will conduct end-to-end testing and confirm to the Buyer when the Service is ready for use.

4. Exit Management Plan

- 4.1. Whether the Buyer would like to cease or move their services to a new provider entirely, Vodafone's Exit Management plan is outlined below;
- a) The Buyer will notify Vodafone of its plan to cease or migrate away from any service within the minimum termination period agreed within the call off-contract.
 - b) Vodafone will extract a contract end date report which will detail the current account set up and any applicable termination fees that will apply to the Buyers final invoice.
 - c) Upon formal request from the Buyer, Vodafone, where applicable, will generate relevant authorisation/ decommissioning codes within applicable Law and regulation and within the regulatory time period.
 - d) The Buyer will manage their relationship and migration plan with their new supplier and, if applicable, share any relevant data provided by Vodafone to their new supplier

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector****5. Service Level Agreement**

5.1. For the purposes of this Service Offer:

- a) The provisions of this Service Level Agreement are compliant with the Service Maintenance Level 1 as set out in Schedule 14 of the Call-Off Terms.

5.2. Vodafone Tiered Support Service Model

- a) In addition to the Service Level Agreement in Service Maintenance Level 1 as set out in Schedule 14 of the Call-Off Terms the Buyer will also benefit from the following additional Tiered Support Service Model ("TSSM") as part of the Service,

- i) Service Request Fulfilment Support Services:

A) Response and Acknowledgement

Deliverable	Contact Method	SLT
Vodafone Initial Response	Email	Near Instant

- ii) Incident Management Support Services:

A) Incident Management Response and Acknowledgement:

Deliverable	Contact Method	SLT
Vodafone will provide the means to report an Incident and provide an Initial Response by the same means.	Telephone	90% of calls answered <20 seconds

- iii) Incident Management Diagnosis:

Deliverable	Contact Method	SLT
<p>Following an Initial Response and as part of initial diagnosis, Vodafone will:</p> <ul style="list-style-type: none"> determine the Infrastructure Service or Supported System on which the incident has occurred; and determine the perceived impact and urgency of the incident including assessment against the criteria for a BMI <p>Vodafone will route the Incident Record to the appropriate support function for expert diagnosis and subsequent management.</p>	Telephone	<30 minutes
Vodafone will contact the party raising the incident to confirm Resolution and closure.	Telephone	<24 hours from Resolution
Vodafone will provide incident updates for each Impact 1 Incident	Telephone	Initial update within 1 hour. Thereafter minimum of hourly or as agreed
Vodafone will provide incident updates for each Impact 2 Incident	Telephone	Initial update within 1 hour. Thereafter minimum of hourly or as agreed

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector**

iv) Buyer Major Incident Management

Deliverable	Contact Method	Premium SLT
Vodafone will attend a conference call on request for a BMI that is in progress	Telephone	15 minutes from receipt of request (subject to the Buyer Site being included in the key site list).
Vodafone will provide enhanced structured Incident updates for BMIs	Telephone	Initial update ≤1 hour, minimum of every 30 minutes thereafter or as agreed
Vodafone will provide a Major Incident high level executive summary, after the Incident is resolved	Telephone	2 Working Days
Vodafone will provide a full BMI report, after RCA of the Incident has been resolved	Telephone	5 Working Days
Volume of Buyer Sites that require BMI	Telephone/email	10% of Buyer Sites

v) Financial Management (Billing) Support Services:

A) Billing Queries:

Deliverable	Contact Method	SLT
Vodafone will provide the means to raise billing queries and provide an Initial Response via email	Email	Near Instant
Vodafone will ensure that all billing queries received via email are Acknowledged	Email	<24 hours

B) Performance Reports

Deliverable	Enhanced SLT
Vodafone will provide scheduled account billing reviews.	Quarterly

vi) Operational Change Management Support Services

- A) A Vodafone-designated "Change Manager" will be responsible for changes and the change management process established by Vodafone from time to time. The Change Manager may be from Vodafone, Buyer or a third party, dependent upon where Vodafone (acting reasonably) determines that responsibility for change governance resides.

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector**

B) Notification of Planned and Essential Operational Changes:

Deliverable	Contact Method	SLT
Vodafone will provide notification of a Planned Outage	Email	10 Working Days
Vodafone will notify Buyer in advance, where reasonably possible, of the scheduling of an Essential Outage	Email	>48 hours

C) Change Schedule Provision

Deliverable	Contact Method	Enhanced SLT
Vodafone will provide and maintain a Change Schedule	Email	Weekly

D) Change evaluation and Support

Deliverable	Contact Method	Enhanced SLT
Vodafone will ensure that all normal operational changes proposed by Buyer, to be delivered by Vodafone are evaluated against the Service referred to in the request by the Buyer and not against multiple Services (unless expressly requested by the Buyer), as provided by Vodafone under the Call-Off Contract to ensure risks have been managed.	Telephone and email	No SLT

vii) Problem Management Support Services

A) Initial Response, Acknowledgement and Routing

Deliverable	Contact Method	Premium SLT
Vodafone will provide the means to report a Problem and provide an Initial Response by the same means.	Email	Near Instant
Vodafone will validate the request for a Problem Record. If the request is valid create a Problem Record and provide an Acknowledgment.	Email	95% <4 Working Hours from receipt
Vodafone ensure all Problems are routed to the appropriate technical or problem management team for Resolution	N/A	No SLT

B) Problem Root Cause Analysis ("RCA") Requests

Deliverable	Contact Method	Premium SLT
Vodafone will carry out RCA on all Impact 1 Incidents	N/A	95% <20 Working Days
Vodafone will carry out Buyer specific basic trend analysis of closed Incidents	N/A	Service not available
Vodafone will carry out Buyer specific in-depth trend analysis of closed Incidents	N/A	No SLT
Vodafone will coordinate RCA investigation of BMIs	N/A	90% <10 Working Days

C) Problem and Incident Trend Analysis Reporting and Review

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector**

Deliverable	Contact Method	Premium SLT
On request Vodafone will provide an initial problem analysis report for those Impact 1 incidents that have repeated 3 times in any 28 day period.	Email	5 Working Days
On request Vodafone will provide an Incident RCA report which includes either the root cause found or an action plan to determine the root cause where reasonably possible for Impact 1 incidents that have repeated 3 times in any 28 day period.	Email	5 Working Days
As part of the “enhanced problem management reports pack” Vodafone will provide a high level trend analysis report.	Email	Service not available
As part of the “premium problem management reports pack” Vodafone will provide a low level trend analysis report.	Email	Monthly
As part of the “enhanced problem management reports pack” Vodafone will provide a Problem Record status report.	Email	Service not available
As part of the “premium problem management reports pack” Vodafone will provide a Problem Record status report.	Email	Weekly

D) Problem Management reviews: Problem and Incident Trend Analysis and Reporting

Deliverable	Contact Method	Premium SLT
Vodafone will provide Problem Record status report review meetings (the problem status report review meeting will only take place if there are any open cases).	Telephone	Weekly

viii) Service Level Management**A) Performance Reports**

Deliverable	Contact Method	Premium SLT
Vodafone will create mid level reports detailing the report's format, content and SLT performance for publication of those reports for each Service that Vodafone provides	Portal/Email	Service not available
Vodafone will create in-depth Reports detailing the report's format, content and SLT performance for publication of those reports for each Service that Vodafone provides	Portal/Email	No SLT

B) Vodafone Service Level Management Team

Deliverable	Contact Method	Premium SLT
Vodafone will provide analysis of performance reports to identify trends, and areas for improvement in the Infrastructure Services and Tiered Support Services being provided and reported on.	N/A	10 Working Days after Reporting Period
Appropriate findings resulting from analysis will be addressed in a service development plan.	N/A	Quarterly
Vodafone will provide performance review meetings with Vodafone service management resource.	Telephone	Service not available
	In person	Monthly
	Telephone (third party to Buyer)	Service not available

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector**

Deliverable	Contact Method	Premium SLT
Vodafone will either itself or via an independent third party continually measure Buyer satisfaction with interactions from a sample of all customers	Telephone	Quarterly
Vodafone will provide service improvement plans as are reasonably required to facilitate improvement where it is needed (at Vodafone's discretion, acting reasonably).	N/A	No SLT
Vodafone will maintain and update a customer support services handbook as it deems required.	N/A	Quarterly
Vodafone will work with Buyer to produce and maintain a service development plan.	N/A	Quarterly

C) Business Relationship Management

Deliverable	Contact Method	Premium SLT
Vodafone will provision regular sector review meetings with a senior manager and Buyer's account manager	In person	Quarterly
Vodafone will provision regular futures review meetings with its nominated subject matter expert(s), senior operational manager(s) and Buyer's account manager	In person	Bi-annually
Vodafone will provision and maintain a risk register relating to Services provided by Vodafone under these Tiered Support Service Specific Terms and conduct regular reviews and analysis of the risk register with Buyer	In person	Bi-annually

ix) Service Request Catalogues

- A) Vodafone may make one or more "Service Request Catalogues" available to Buyer through its online portal at OnePortal ("Portal"). A URL for the Portal will be provided to the Buyer via the support handbook. Service Request Catalogues contain information about the Tiered Support Services and Service Requests, including those Service Requests that will be self-served by the Buyer and those that will be serviced by Vodafone, broken down by Service.
- B) Any Service Request Catalogue information made available to Buyer is provided for guidance only; it is not binding on Vodafone and does not form part of this Agreement.
- C) Vodafone may change the information contained in the Service Request Catalogue at its discretion, via a catalogue update, provided that the changes do not materially affect the nature of the Tiered Support Services delivered to Buyer.

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services**

Vodafone Dedicated Internet Access

Public Sector

**6. Optional Schedules**

This Service Offer assumes that the Buyer is not electing to take any of the following Optional Schedules;

- 6.1. Call-Off Schedule 4 of the Call-Off Contract shall not apply.
- 6.2. Call-Off Schedule 6 of the Call-Off Contract shall not apply.
- 6.3. Call-Off Schedule 7 of the Call-Off Contract shall not apply.
- 6.4. Call-Off Schedule 10 of the Call-Off Contract shall not apply.
- 6.5. Call-Off Schedule 13 of the Call-Off Contract shall not apply.
- 6.6. Call-Off Schedule 15 of the Call-Off Contract shall not apply.
- 6.7. Call-Off Schedule 16 of the Call-Off Contract shall not apply.
- 6.8. Call-Off Schedule 17 of the Call-Off Contract shall not apply.
- 6.9. Call-Off Schedule 18 of the Call-Off Contract shall not apply.
- 6.10. Call-Off Schedule 22 of the Call-Off Contract shall not apply.
- 6.11. Call-Off Schedule 23 of the Call-Off Contract shall not apply.
- 6.12. Call-Off Schedule 24 of the Call-Off Contract shall not apply.
- 6.13. Call-Off Schedule 25 of the Call-Off Contract shall not apply.
- 6.14. Joint Schedule 6 of the Call-Off Contract shall not apply.
- 6.15. Joint Schedule 7 of the Call-Off Contract shall not apply.
- 6.16. Joint Schedule 8 of the Call-Off Contract shall not apply.
- 6.17. Joint Schedule 9 of the Call-Off Contract shall not apply.
- 6.18. Joint Schedule 12 of the Call-Off Contract shall not apply.

Should the Buyer wish to take any of the above schedules, then these may be subject to additional charges. Please contact your Vodafone account manager, or frameworks_team@vodafone.com who will clarify your requirements, and where needed publish a new Service Offer containing the selected Optional Schedules.

7. Mandatory Schedules

- 7.1. In accordance with the Supplier's obligations under any Call-Off Contract, Vodafone has developed and will maintain the following reports and plans, which are available to view, download, print or save, on Vodafone's Public Sector Portal. By entering into a Call-Off Contract Buyer confirms that it accepts the following reports and plans as is, with no alteration:
 - a) Call-Off Schedule 1 (Transparency Reports) - Transparency Report in accordance with Call-Off Schedule 1.
 - b) Call-Off Schedule 8 (Business Continuity and Disaster Recovery) – Business Continuity and Disaster recovery Plan in accordance with Call-Off Schedule 8.
 - c) Call-Off Schedule 9 (Security) - Security Management Plan in accordance with Call-Off Schedule 9. The Security Management Plan for any Deliverables purchased under this Service Offer shall be the Supplier's Security Management Plan published on Vodafone's Public Sector Portal. By entering into a Call-Off Contract the Buyer acknowledges and agrees:

RM6116 Network Services 2



Lot 1a – Inter site Connectivity / Data Access Services

Vodafone Dedicated Internet Access

Public Sector

- i) the Supplier has prepared and delivered the Security Management Plan (published as set out above) to the Buyer; and
- ii) the Buyer has approved the Security Management Plan, in accordance with Call-Off Schedule 9 (Security) Part A: Short Form Security Requirements.

8. Service Description and Price Card

8.1. Primary Services

The Vodafone Dedicated Internet Access Services provide Buyer with symmetrical access to the public internet either over dedicated access bearers, shared access bearers, or directly to Vodafone's IP-VPN network. The Service is provided using the Global Vodafone IP Backbone or a combination of the Global Vodafone IP Backbone and the Vodafone Global IP-MPLS Networks. The term "Service" or "Services" in these Service Specific Terms means the Internet Access Services (as further detailed in the Service Specification).

Wires Only – Buyers have the option of a 12, 24 or 36-month term.

Dedicated Symmetrical Access Circuits - Buyers do not have to share their bandwidth with anyone else. Buyers receive all the bandwidth that they are paying for. Symmetrical circuits allow Buyers to utilise the full available bandwidth for either upstream or downstream traffic. There are no restrictions on monthly usage or additional charges for large files.

Choice of access connectivity - Fibre-based Ethernet, connections at any of the standard 100Mbps, 1000Mbps or 10Gbps speeds. The Dedicated Internet Access Service can be provided at a range of lower 'throttled' speeds, so Buyers only pay for the bandwidth provided. The Buyer can take the higher bandwidth when the Buyer's requirements change. Buyers are able to order the following committed bandwidth combinations;

Buyer Premise Equipment (BPE) (i.e. Routers) – where ordered these will be installed, configured, managed and maintained by Vodafone. BPE and other devices inherit the physical controls of the Buyer environment in which they are installed. In addition to these physical controls, additional controls are deployed to help mitigate the risks associated with power (feeds, power distribution units, UPS or equivalent backup generators) and cabling security (e.g. change management, dual routing, cable labelling, tidy & careful cabling to documented standards (e.g. avoids bends, kinks), use of ducting and where possible enclosed metal or clear conduit. There are three types of BPE a Buyer can rent;

- a) Low – Router hardware capable of supporting the requested VPN (port) throughput bandwidth as measured using an IMIX traffic profile
- b) Medium – Router hardware capable of supporting the requested VPN (port) throughput bandwidth as detailed in the router pricing section.
- c) High – Router hardware capable of offering a higher service performance and supporting upgrades in VPN (port) bandwidth without a change in router hardware. Premium router hardware shall be capable of supporting the maximum VPN (port) bandwidth possible on the chosen access connectivity based on a IMIX traffic profile. Premium router hardware should be selected where there is a requirement for a small average 64 Byte packet size (such as for large IP Voice traffic usage)

Access Circuit Bandwidth	Committed Service Bandwidths	Committed + Burst Service Bandwidths (Global IP-MPLS Access types only)	Access Technology	Interface (Buyer Provided Router)
100Mbps	10, 15, 20, 30, 40, 50, 60, 70, 80, 90, 100Mbps	10Mbps burst to 20Mbps 20Mbps burst to 40Mbps 50Mbps burst to 100Mbps	Ethernet	RJ45

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector**

Access Circuit Bandwidth	Committed Service Bandwidths	Committed + Burst Service Bandwidths (Global IP-MPLS Access types only)	Access Technology	Interface (Buyer Provided Router)
1000Mbps	100, 200, 250, 300, 400, 500, 600, 700, 800, 900, 1000Mbps	100Mbps burst to 200Mbps 200Mbps burst to 400Mbps 500Mbps burst to 1000Mbps	Ethernet	1000Base SX/LX
10Gbps	1, 1.5, 2, 2.5, 3, 3.5, 4, 5, 6, 7 & 10Gbps	N/A	Ethernet	10G LAN PHY

- Ethernet circuits may be provided on fibre or copper access technology
- Burst options only available where DIA delivered over dedicated access bearer
- Service bandwidths are inclusive of all protocol & access network transmission overheads

Managed Only Service – 24 Month Term

Site	Primary / Secondary	Postcode	Service Speed / Bandwidth	Router	One off Charges - NRC	Monthly Charge (£) MRC	Annual Charge (£) ARC
Stratford Redman Place	Primary	NE1 4WH	50 MB / 100 MB	C1117-4P (#1117-4P-0-AC)	£ 846.15	£ 1,073.25	£ 12,878.97
Stratford Redman Place	Secondary	NE1 4WH	50 MB / 100 MB	C1117-4P (#1117-4P-0-AC)	£ 846.15	£ 1,133.74	£ 13,604.91
Newcastle City Gate	Primary	E20 1JQ	800 MB / 1000 MB	C8200L-1N-4T (#8200L-1N-4T-0-AC)	£ 846.15	£ 622.73	£ 7,472.82
Newcastle City Gate	Secondary	E20 1JQ	800 MB / 1000 MB	C8200L-1N-4T (#8200L-1N-4T-0-AC)	£ 846.15	£ 851.50	£ 10,217.96

Performance Reporting (Per Site)

To help the Buyer better understand how the Service is meeting their internet traffic needs. The table below outlines the pricing for Performance Reporting services per Buyer Site.

Performance Reporting per Site		
Term	NRC	ARC
1-year term	£-	£413.76
2-year term	£-	£242.12
3-year term	£-	£184.91

Internet Features

- Public IP Addresses

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector**

- Domain Name Transfer and Registration

The table below outlines the pricing for the Internet Features available:

Public IP Addresses		
Quantity	NRC	ARC
Per Block of 48	£ 90.00	£ 106.00

Domain name registration Price Per Unit		
Type	NRC	ARC
UK	£ -	£ 108.00
COM	£ -	£ 216.00
ORG	£ -	£ 108.00
GOV	£ -	£ 108.00
AC	£ -	£ 108.00

Domain Name Transfer Price Per Unit		
Type	NRC	ARC
UK	£ -	£ 108.00
COM	£ -	£ 216.00
ORG	£ -	£ 108.00
GOV	£ -	£ 108.00
AC	£ -	£ 108.00

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector****8.2. Ancillary Services**

Ancillary Charges associated with services provided by a third party /OLO

Unless otherwise agreed and stated in the Buyer's Call-Off Contract, the Buyer will be liable for any additional costs charged to Vodafone by third parties in connection with the provision of the Services. Such Charges include but are not limited to the following:

Feature	Single Payment Charge £ Exc VAT	Connection Charge £ Ex. VAT
Survey Fee/ Planning Charge (Previously included in other charges) This item will only be charged if Excess Construction Charges are accepted by a Buyer except for Non-Standard Lines where the Survey Fee will be charged with every order. It will be included as an item within the excess charge's calculation and each resurvey additional to the first survey will increment the cost by a further £244.52	£244.52	
Breaking/Drilling through each external wall	£85.94	
Breaking/Drilling through each internal concrete wall	£120.69	
Breaking/Drilling through each internal non-concrete wall	£21.26	
Provision of each Pole	£419.68	
Provision of a new footway box (Surface area up to 0.5 sqm)	£771.36	
Provision of a new medium size footway box (Surface area between 0.5 sqm and 1 sqm)	£1,383.01	
Provision of a new large size footway box (Surface area greater than 1 sqm)	£2,708.03	
Provision of a new small carriageway box (Surface area up to 1 sqm)	£2,197.23	
Provision of a new medium size carriageway box (Surface area between 1 sqm and 1.25 sqm)	£3,539.18	
Provision of a new large size carriageway box (Surface area greater than 1.25 sqm)	£4,603.13	
Cable (fibre or copper) including any jointing required (per metre)		£7.53
Copper cable supplied for the Buyer to lay to agreed entry and termination points (per metre). (minimum 20m supply) This charge includes on site termination and jointing work by Openreach to connect and terminate the cable. If the order is for less than 40 metres then a visit charge will apply - Please See Visit Charges for details.		£4.33
Directly buried cable (including any cable and wayleave costs) (per metre)		£22.50
Moleploughing cable or fibre in subduct (includes any cable and wayleave costs) (per metre)		£11.00
Blown Fibre (per metre)		£1.74
Blown Fibre Tubing in Duct (per metre)		£3.83
Fibre Cable (per metre)		£5.51
Internal cabling (including Internal Blown Fibre Tubing) (per metre)		£7.42
New Ductwork - Softsurface (includes wayleave costs) (per metre)		£32.29
New Ductwork - Footway (includes wayleave costs) (per metre)		£66.55
New Ductwork - Carriageway (includes wayleave costs) (per metre)		£118.63
Trunking and traywork within end-user's curtilage (per metre)		£17.76
Overblow Services (per 100 metres)		£364.83

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector**

Site Visits by Vodafone

Additional site visits requested by the Buyer or abortive site visits will be charged as per the following table;

Ancillary Charge per visit	Description	Working Hours	Out of Normal Working Hours A *	Out of Normal Working Hours B **
Site Visit	Buyer Site Visit required or requested (a Site Visit not identified in the Call-Off Contract)	£350	£500	£650
Aborted Site Visit†	Vodafone's engineer Site Visit for an appointment but cannot gain access to do the work required or the site has not been appropriately prepared as per Vodafone instructions	£350	£500	£650
Site Survey	Additional Site Survey	£500	£700	£900
Extended Site Visit	Should the engineer need to extend the period on-site for any Buyer related reason additional charges will be incurred e.g., Access delays, non-adherence to Vodafone instructions	£58/hr or part thereof	£82/hr or part thereof	£106/hr or part thereof
Buyer site visit Fault/Incident outside of Vodafone domain†	Buyer Site Visit to investigate a reported Fault/Incident, which transpires to be outside the domain of the services provided by Vodafone. (e.g services provided by the Buyer or its Third-Party Providers).	£350 for the first 3hrs + £58/hr or part thereof	£500 for the first 3hrs + £82/hr or part thereof	£650 for the first 3hrs + £106/hr or part thereof
Cancelled Site Visit	Buyer caused cancellation of engineering Site Visit Note: No Charge if cancelled more than 48 hours before the scheduled appointment	Within 24hrs of Site Visit = full aborted Site Visit charge Between 24 and 48hrs of Site Visit = 50% of aborted Site Visit charge		

* (any time outside of normal Working Hours on Monday to Friday and including any time on Saturday but excluding any time within Out of Normal Working Hours B)

** any time on a Sunday or Public Holiday in the UK)

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector****Professional Services**

Vodafone offer a range of professional services including technical consultancy, project management and on-site service management.

Charges	
	Maximum daily rates excluding expenses
Consultants	
Junior Consultant	£615
Consultant	£720
Senior Consultant	£850
Principal Consultant	£850
Partner/ Director	£1,000
Contractors / IT Specialists	
Senior Analyst/ Team Leader	£570
Systems Analyst & Designers	£570
Analyst/ Programmers	£570
Application Programmers	£570
System Programmers	£570
Database Administrators	£570
Network Administrators	£430
Capacity Planners	£475
Configuration Managers	£475
IT Trainers	£475
Documentation Specialists	£380
Project Administrators	£475

9. Key Sub-Contractors

- Openreach Limited
 - Kelvin House, 123 Judd Street, London, United Kingdom, WC1H 9NP
 - 10690039
- Virgin Media Limited
 - Media House, Bartley Wood Business Park, Hook, Hampshire, RG27 9UP
 - 02591237
- CityFibre Limited
 - 15 Bedford Street, London, England, WC2E 9HE
 - 09759465

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector****10. Definitions**

The following definitions are applicable to this Service Offer;

Access Circuit	a circuit which connects a Buyer Site to the Global IP-MPLS Network and onwards to an Internet Edge Router on the Vodafone IP Backbone or connects directly between the Buyer Site and an Internet Edge Router.
Acknowledgement	a confirmation given to Buyer that a particular request or Incident raised is valid and the provision to Buyer of a unique reference for it. "Acknowledge" shall be construed accordingly.
Additional Service Recipients	a Buyer Group entity which is not a direct party to this Agreement, but which is named in this Agreement as a beneficiary of the Services or otherwise approved to receive the Services
Agreement	means the Call-Off Contract and Service Offer.
Annual Measurement Period	the period of twelve (12) months from the Service Commencement Date or each anniversary of the Service Commencement Date thereafter (or a period of twelve months as otherwise agreed between the parties).
AUP	Vodafone's acceptable use policy available on request.
Black Hole	to Black Hole traffic (aka Black Holing) is to drop that traffic before it reaches its destination. Typically, purposely done to avoid Denial of Service at the destination.
BMI	a "Buyer major incident", being the highest category of Impact for an Incident resulting in significant disruption to the business of Buyer.
Burst Service Bandwidth	an amount of Service Bandwidth that Vodafone shall use reasonable endeavours to provide to Buyer.
Buyer Equipment	hardware, Software, or any other tangible material not supplied by Vodafone that is used with or to access the Service. Any Equipment Buyer purchases from Vodafone shall be considered to be Buyer Equipment once title has passed to the Buyer.
Buyer Domain Name	the meaning set out in the Service Offer.
Buyer Edge Router	a router to which the Access Circuit is connected at a Buyer Site.
Buyer Group	Buyer and any company in which Buyer has the beneficial ownership of more than 50% of the issued share capital, or the legal power to direct the general management of the company in question, either at or after the date of the Call-off Contract.
Buyer Provided Router	a Buyer Edge Router at a Buyer Site that has been provided by Buyer and is used with the Service and which is managed by Buyer or by another service provider. The Buyer Provided Router is not owned by Vodafone.
Buyer's Service Desk	is the service desk provided by Buyer which will be the initial point of contact between Vodafone and Buyer.
Buyer Site	as the context permits a Buyer's premises (either owned by Buyer or a third party) which Vodafone needs to access in order to deliver or install Equipment and/or to provide the

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector**

	Services or the location where the Services are to be provided, as set out in the Call-Off Contract.
	a document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a “forward schedule of change”.
Committed Service Bandwidth	an amount of Service Bandwidth that Vodafone commit to provide to Buyer.
Configuration Changes	Hard Configuration Changes and/or Soft Configuration Changes.
BPE (Buyer premises equipment)	Fixed Equipment on Buyer Site.
DNS	Domain Name Service and has the meaning set out in the Service Specification.
End Of Life	where Vodafone or a manufacturer of Equipment declares that the type of Equipment is end-of-life (or otherwise stops marketing, selling or supporting it).
Equipment	hardware, Vodafone Software, and any other tangible equipment (other than SIMs) supplied by, or on behalf of, Vodafone to Buyer for use in receiving the Services. Equipment excludes Buyer Equipment.
Essential Outage	an Outage that is not a Planned Outage including, but not limited to, Outages caused by a force majeure event or an act or omission of any third party which is beyond Vodafone's reasonable control.
Existing Global IP-MPLS Network Access Bearer	means a last mile connection into the Buyer Site from Vodafone's MPLS point of presence.
Fixed Equipment	hardware, Vodafone Software, BPE and any other tangible equipment (other than SIMs and mobility equipment) supplied by or on behalf of, Vodafone to Buyer for use in receiving the Services.
Fully Diverse	means two BPE with two access tails that connect to two different multi service provided edge (“MSPE”) nodes, which backhaul to two different IER nodes.
Global IP-MPLS Network	the private, MPLS based, network with underlying transport owned by Vodafone.
GSM Gateway	any equipment containing a SIM card which enables the routing of calls from fixed apparatus to mobile equipment by establishing a mobile to mobile call.
Hard Configuration Change	a change to the Internet Access Services provided to Buyer that may include one or more of the following: <ul style="list-style-type: none"> (a) transfer of service from one Buyer Site to another; (a) migrating between physical Access Circuit options; (b) modifications requested by Buyer to alter the Internet Access Services at a Buyer Site requiring physical intervention; (c) physical movement of a Buyer Site; or (d) the cessation of an Internet Access Service at a Buyer Site.
Helpdesk(s)	the Buyer Services Helpdesk

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector**

	a measure of the effect of an incident, problem or change on business processes. impact is often based on how service levels will be affected. Impact and urgency are used to assign priority.
Incident	any fault or problem which affects the Internet Access Services provided to Buyer, which is not: (i) an Excluded Event, (ii) a result of an Outage, (iii) a failure at another Buyer's Site; (iv) a failure in relation to Third Party Provider Supplied Internet Access Services; (v) any failure of the BSE/BPE; or (vi) failure in relation to a Third Party Provider Supplied Internet Access Services (vii) an unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected Service is also an Incident.
Incident Record	a record containing the details and lifecycle of an Incident.
Infrastructure Services	an IT service that is not directly used by Buyer's business but is required for the provision of other IT services (for example either a Functional Service, connectivity service, hosting service or any combination thereof).
Initial Response	a first response from Vodafone to an individual raising a request or Incident, such as answering the telephone or replying to an email.
Internet Edge Router ("IER")	a router on the Vodafone IP Backbone to which an Access Circuit connects to either directly or once it has traversed the Global IP-MPLS Network.
IP Address	a numerical label that is assigned to any device participating in a computer network that uses the public internet for communication between its nodes
Managed	the Service package where Vodafone supplies, installs, maintains and manages the managed Vodafone Supplied Router as further outlined in clause 3.6 of these Service Specific Terms and the Service Specification.
Network	the communications network together with the equipment and premises that are connected to such network and which are used by Vodafone to perform the Services.
Network Based Internet Access	the delivery of Internet Access to a Buyer via a Secure Network Gateway to a Buyer's Vodafone provided IP-VPN Service.
Network Latency	as described in Annex 1.
Network Termination Equipment" or "NTE"	a device used to terminate Buyer's connection where Buyer has Ethernet access.
Outage	a temporary and unavoidable interruption in service, which is necessary for Vodafone to carry out essential maintenance or network upgrades.
Packet Loss	as described in Annex 1.
Planned Outage	the scheduled unavailability of an Infrastructure Service.
Primary IP Backbone Nodes	a specific node on the Vodafone IP Backbone as identified by Vodafone from time to time and notified to Buyer.
	a cause of one or more Incidents. The cause is not usually known at the time a problem record is created, and the problem management process is responsible for further investigation.

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector**

	a record containing the details and lifecycle of a Problem.
Resolution	the exercise by Vodafone of its reasonable endeavours to repair the root cause of an Incident or Problem, or to implement a workaround.
Router	a router that is used in connection with the Service which may be either a Managed Vodafone Supplied Router or a Buyer Provided Router.
Secure Network Gateway	the infrastructure used to provide Network Based Internet Access in conjunction with a Vodafone IP-VPN service. The Secure Network Gateways are connected to Vodafone's IP Backbone and Global IP-MPLS network.
Services	the Vodafone product(s) detailed in this Service Offer.
Service Bandwidth	the level of bandwidth that may be available to Buyer, which can be Committed Service Bandwidth or Burst Service Bandwidth.
Service Commencement Date	the date of completion of Vodafone's testing when the Service is ready for use.
Service Demarcation Point	the access interface on the Managed Vodafone Supplied Router or Access Circuit.
Service Element	the individual components of a Service (including optional service elements if applicable), such as the individual access circuits.
Service Request	a request from a user for information, or advice, or for a Standard Change or for access to an IT service made in accordance with the requirements of the relevant Service Request Catalogue.
Site Survey	a survey of a Buyer's Site to assess whether (in Vodafone's opinion) the existing infrastructure is sufficient for providing the Services and detailing what the Buyer needs to do to receive the Service.
Soft Configuration Change	a change to the Internet Access Services provided to Buyer that does not constitute a Hard Configuration Change, including, without limitation, the following: <ul style="list-style-type: none"> a. modifying or providing new IP Addresses; or modifying the Committed Service Bandwidth provided over an Access Circuit.
Standard Change	a pre-approved Change that is low risk, relatively common and follows a procedure or work instruction. The types of Standard Changes available are listed in a Service Request Catalogue.
Supplier	where used in this Service Offer or Call-Off Contract means Vodafone
Third Party Provider	a Key Subcontractor or third party contracted by Vodafone or Buyer that provides a Service, or that provides a service that connects to a Service.
Tiered Support Service Model or TSSM	the tiered support services provided by Vodafone in accordance with the service level agreement set out herein.
User	an individual end user of the Services who is approved by Buyer and who must be a permanent or temporary employee or sub-contractor of Buyer or an Additional Service Recipient unless otherwise specified in this Agreement.

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access**

Public Sector



User Details	a user name, password, or other access information used by a User to access the Service and/or Equipment.
Vodafone IP Backbone	is collectively represented by Vodafone autonomous system Networks known as AS1273, AS6660 and AS2529.
Vodafone Software	any Software supplied by Vodafone or its licensors to Buyer (including Software embedded in any Equipment).
Vodafone Supplied Router	a Buyer Edge Router at a Buyer Site that is provided and Managed by Vodafone.
Wires Only	Buyer supplies, installs, maintains and manages the Buyer Provided Router.
Working Days	Monday to Friday inclusive, other than public holidays in the UK.
Working Hours	the hours between 8.00am and 6.00pm on each Working Day.

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector****Annex 1 – Dedicated Internet Access Availability**

Service Configuration at relevant Buyer Site	Percentage availability at the Service Demarcation Point of each Buyer Site (P)
Single Service	99.90%
Dual Parent (Diverse Internet Edge Routers)	99.95%
Dual Parent (Fully Diverse)	100%
<p>Calculation:</p> <p>Service availability at the Service Demarcation Point for each Buyer Site will be calculated as follows:</p> $P = \frac{A - B}{A} \times 100\%$ <p>where:</p> <p>P = percentage availability</p> <p>A = number of minutes in the relevant Annual Measurement Period</p> <p>B = number of whole minutes during which the Internet Access Services are Unavailable in the Annual Measurement Period, excluding time where the Internet Access Services are Unavailable due to: (i) Outages; (ii) an Excluded Event; (iii) a failure at the other Buyer Site; (iv) a failure in relation to a Third-Party Provider Supplied Internet Access Service or (v) any failure of the BSE/BPE.</p> <p>This Availability Service Level only applies to Internet Access Services provided at those Buyer Sites directly connected to Vodafone's Global IP-MPLS Network or Internet Edge Router. The Availability Service Level does not apply to Third Party Provider Supplied Internet Access Services or Network Based Internet Access.</p> <p>This Availability Service Level is measured as the percentage of time the Internet Access Service is available at the Service Demarcation Point of each Buyer Site in an Annual Measurement Period.</p> <p>Unavailable or Unavailability means a Buyer Site cannot access the Vodafone IP Backbone, unless the unavailability arises out of, or in connection with, any of the following:</p> <ol style="list-style-type: none"> an Outage; an Excluded Event; a failure at the other Buyer Site; or any failure of the BSE/BPE. <p>The period of Unavailability shall be measured in accordance with the Incident Commencement and Resolution Rules set out in clause 1.3 above.</p>	

RM6116 Network Services 2**Lot 1a – Inter site Connectivity / Data Access Services****Vodafone Dedicated Internet Access****Public Sector****Service Degradation**

Monthly average Network Latency and Packet Loss Service Levels		
Region	Parameters	Service Level target
Europe	Network Latency (ms)	35
	Packet Loss (%)	0.2
Europe UK	Network Latency (ms)	20
	Packet Loss (%)	0.2
Europe North America	Network Latency (ms)	90
	Packet Loss (%)	0.2
Europe Asia	Network Latency (ms)	310
	Packet Loss(%)	0.2
UK	Network Latency (ms)	35
	Packet Loss(%)	0.2
UK North America	Network Latency (ms)	90
	Packet Loss (%)	0.2
UK Asia	Network Latency (ms)	210
	Packet Loss (%)	0.2
North America	Network Latency (ms)	65
	Packet Loss (%)	0.2
North America Asia	Network Latency (ms)	165
	Packet Loss(%)	0.2
Asia	Network Latency (ms)	90
	Packet Loss(%)	0.2

This Service Degradation Service Level applies to the Network Latency and Packet Loss performance of the Vodafone IP Backbone. The Service Degradation Service Level does not apply to Third Party Provider Supplied Internet Access Services.

Network Latency - measures the amount of time that it takes for data to travel between specific Primary IP Backbone Nodes, and back, on the Vodafone IP Backbone within each Region and between Regions.

The Service Level performance for Network Latency will be calculated as follows: (i) within a Region - by taking an average of the average monthly Network Latency performance for all routes between Primary IP Backbone Nodes within that Region; and (ii) between two Regions - by taking the monthly average Network Latency of the two Primary IP Backbone Nodes with the lowest Network Latency between those Regions.

Packet Loss measures the percentage of data that is lost during the transit of data between specific Primary IP Backbone Nodes on the Vodafone IP Backbone within each Region and between each Region.

The Service Level performance for Packet Loss will be calculated as follows: (i) within a Region detailed above - by taking an average of the average monthly Packet Loss performance for all routes between Primary IP Backbone Nodes within that Region; and (ii) between two Regions - by taking the monthly average Packet Loss for all routes between Primary IP Backbone Nodes between those Regions.

The Service Level targets for Network Latency and for Packet Loss may vary from time to time. Vodafone will notify Buyer when this happens. Changes to these targets that are beneficial to Buyer, (ie where the target increases), will apply as soon as Vodafone announce them. In all other circumstances the changes shall apply with effect from such date as Vodafone may notify to Buyer, or if Vodafone has not notified Buyer of such a date then they shall apply automatically from the start of the following Renewal Term.



vodafone
business

Together we can

RM6116 - Network Services 3

Service Offer Reference: RM6116-Lot2a-VodafoneLtd-#020

Lot(s): 2a

Effective Date: 12/06/2025

Expiry Date: 20/07/2025





RM6116 Network Services 3
Lot 2a - Intra Site Connectivity
Vodafone Local Area Network (including Wi-Fi)
Public Sector

Contents

<u>1.</u>	<u>The Service – Overview and why Vodafone</u>	3
<u>2.</u>	<u>Conditions on the Buyer</u>	3
<u>3.</u>	<u>Outline Implementation Plan</u>	8
<u>4.</u>	<u>Exit Management Plan</u>	8
<u>5.</u>	<u>Service Level Agreement</u>	8
<u>6.</u>	<u>Optional Schedules</u>	11
<u>7.</u>	<u>Mandatory Schedules</u>	11
<u>8.</u>	<u>Service Description and Price Card</u>	12
<u>9.</u>	<u>Key Sub-Contractors</u>	26
<u>10.</u>	<u>Definitions</u>	26



RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector

1. The Service – Overview and why Vodafone

- 1.1 Vodafone's wired and wireless Local Area Network (LAN) solution give users secure and reliable access to business systems and resources from any device.

A local area network (LAN) is a network that interconnects computers within a limited area such as a home, office building or warehouse. A LAN will interconnect to a Wide Area Network (WAN) or the internet by an external fixed communications line.

Ethernet and Wi-Fi are the two most common transmission technologies in use for local area networks.

Vodafone's technology partner of choice is Cisco (including Meraki), who are recognised as a market leader in wired and wireless LAN technology.

Under this Service Offer, Buyers may take the hardware devices that form the LAN and in addition may take one of the incremental Service Wraps.

- 1.2 Vodafone provides you with Local Area Network (LAN) connectivity services and/or Local connectivity services to connect an end user device to a local service (the "Service").
- 1.3 Vodafone LAN and WLAN solutions offer design, implementation, and remote monitoring and end-to-end management for our Buyers. We aim to increase productivity, flexibility, reliability and management workload; for best connected employee, guest and Buyer experience, with enhanced security.

2. General Conditions on the Buyer

- 2.1 This Service Offer is available to Buyers that meet and agree to the following criteria:
- (a) In accordance with Joint Schedule 7 (Financial Difficulties) paragraph 2.2, Joint Schedule 7 (Financial Difficulties) shall not apply to any Call-Off Contract entered into incorporating this Service Offer.
 - (b) **Authorised Users:** Access by Buyer to the Services and Equipment is limited to authorised Users. If Vodafone provides each authorised User with User Details, Buyer is responsible for: (a) the security of the User Details; and (b) providing Vodafone with the identity of the authorised Users and keeping that information current. Vodafone accepts no liability for any unauthorised or improper use or disclosure of any User Details. Buyer is liable for all acts and omissions conducted using the User Details up until the time that it informs Vodafone that they are being used without authority or may be compromised.
 - (c) **Additional Service Recipient:** If Buyer wishes to add Additional Service Recipients, then Buyer shall: (a) provide the full corporate details of the Additional Service Recipient; (b) seek approval in writing from Vodafone; (c) inform the Additional Service Recipient of the contractual arrangements; and (d) agree to pay such additional charges as Vodafone may reasonably request in relation to the approval of such requests.
 - (d) Save as expressly permitted under this Agreement, Buyer shall not resell, distribute, provide or sub-licence the Services or Equipment (except Buyer Equipment) to any third party.
 - (e) Buyer shall take appropriate measures to back up data and otherwise protect against loss of data under this Agreement.
 - (f) **Terms of use:** Buyer shall not (a) make unauthorised modifications to the Services (b) use the Services as a means to establish permanent servers, relay connections or interconnection services or any similar commercial activities, (c) do anything that causes the Network to be impaired; (d) use automated means to make calls, texts or send data (including via a GSM Gateway), unless expressly authorised in this Agreement or (e) use the Services in a way that may reasonably be considered to be a nuisance, defamatory, offensive, abusive, obscene or in violation of any person's rights or is illegal, fraudulent or contrary to good faith commercial practice to Vodafone's detriment. Buyer shall comply with the AUP in using the Services. Buyer shall notify Vodafone immediately of any breach of security or unauthorised use of the Services.



RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector

- (g) Service Monitoring: Buyer gives express consent for Vodafone to monitor Buyer's use of the Service (and disclose and otherwise use the information obtained) only to: (a) the extent allowed by applicable Law; (b) comply with applicable Law; (c) protect the Network from misuse; (d) protect the integrity of the public internet and/or Vodafone's systems and Networks; (e) the extent necessary to determine if Buyer has breached any conditions or restrictions on use of the Service; (f) provide the Service; and/or (g) take other actions agreed or requested by Buyer.
- (h) Security: Buyer shall take reasonable steps in line with commercial good practice with entities it controls to limit misuse of or threat to the Service or Network; and address any misuse or threat identified by Vodafone through the implementation of appropriate security or user controls. Buyer must seek prior approval from Vodafone before running any security tests, vulnerability scans or penetration tests on Vodafone Equipment or Services.
- (i) Buyer acknowledges that Buyer Equipment is not authorised for use on the Network or any unauthorised attempt to repair or tamper with the Equipment may result in an impaired User experience and/or invalidate the manufacturer's warranty.
- (j) Vodafone will not be liable for Buyer's use of Equipment where Buyer has not installed, updated or followed Vodafone's reasonable recommendations regarding Equipment (including for any failures), and Vodafone will also not have any maintenance obligations.
- (k) Equipment that is (i) out of manufacturer's warranty; or (ii) End Of Life is used at the Buyer's risk unless expressly agreed otherwise by Vodafone.
- (l) Buyer must:
 - (i) Appropriately configure its equipment to enable consumption of the Service.
 - (ii) Maintain Buyers Equipment.
 - (iii) Provide details to facilitate the delivery, provisioning and billing of the Services requested by Vodafone at the time of ordering.
 - (iv) Secure and keep in place, or assist Vodafone to obtain (at the Buyer's cost), all relevant third party consents and approvals necessary for the purposes of providing, and preparing for the provision of, the Service. Such consents and approvals include obtaining any necessary wayleave on Vodafone's requirements.
- (m) Where Buyer terminates the Call-Off Contract during the Initial Period, the Buyer agrees to pay Vodafone's reasonable and proven losses resulting from the termination of the Call-Off Contract.

22 Fixed Services Conditions on the Buyer

- (a) Service Commencement Date: Buyer shall notify Vodafone within 5 Working Days of the Service Commencement Date if the Services do not conform to the standard testing criteria and provide sufficient supporting details. Upon receipt of notification, Vodafone shall take reasonable action to meet the standard testing criteria.
- (b) Vodafone-Owned Equipment: The following will apply where Vodafone provides Fixed Equipment for Buyer's use with a Service:
 - (i) Title: Title to the Fixed Equipment at all times belongs to Vodafone, its suppliers or subcontractors (subject only to any rights which may be granted to Buyer in respect of Vodafone Software as set out in this Service Offer).

Buyer Obligations: Buyer agrees to:

- (ii) provide secure storage for Fixed Equipment that is sent to Buyer Sites prior to installation;
- (iii) use the Fixed Equipment only for the purpose of using the Services, in accordance with Vodafone's instructions and applicable Law;
- (iv) allow only Vodafone's authorised representatives to add to, move, modify, inspect, test or alter the Fixed Equipment (either on Buyer Site or remotely);



RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector

- (v) adequately insure for, and notify Vodafone immediately of, loss, breach or suspected breach or damage to the Fixed Equipment;
- (vi) only connect the Fixed Equipment to the Network using a network termination point that has been approved in advance by Vodafone;
- (vii) provide Vodafone with adequate power supply, connection, and space for the operation of the Fixed Equipment at Buyer Sites and in the case of BPE, patch cords and cabling and provide Vodafone 10 Working Days' notice of any known disruptive event (such as power disconnection); and additionally, specifically in relation to BPE:
 - (A) appoint a local security representative to ensure the physical security of the BPE who will grant access by approved authorised personnel only and conduct routine physical checks, including ensuring tamper evident labels remain intact; and
 - (B) ensure that the physical environment in which the BPE is housed is appropriate for the protective marking of the data being transmitted through such Fixed Equipment. In particular, (i) BPE must be located in a communications room or other isolated area that is suitable to limit the occurrence of accidental or malicious damage to the BPE; and (ii) if the BPE is located in a shared environment, then it must be kept in a dedicated locked cabinet or rack. If that is not possible, robust access control mechanisms must be implemented by Buyer, with access only available with prior approval from Buyer's local security representative.
- (c) Buyer Equipment: Where Buyer provides Buyer Equipment for use with a Service Buyer shall (and Buyer acknowledges that failure to do so will excuse Vodafone from liability for failure to deliver the Service):
 - (i) install and configure the Buyer Equipment at the Buyer Sites by the date necessary to allow Vodafone to perform its obligations;
 - (ii) maintain the Buyer Equipment including prompt installation of security patches and updates;
 - (iii) promptly after the Service Offer terminates, give Vodafone access to and reasonable help with disconnecting Buyer Equipment from the Service; and
 - (iv) warrant and undertake that Buyer has full authority to permit Vodafone to perform the Services using the Buyer Equipment
- (d) Buyer Sites: For the purposes of preparing for and delivery of the Services, Buyer shall:
 - (i) carry out, or permit Vodafone or its subcontractors to conduct, a Site Survey;
 - (ii) prepare the Buyer Site for the Services in accordance with Vodafone's instructions;
 - (iii) allow and/or have in place (or assist Vodafone to do so at Buyer's cost) all third party consents necessary to allow Vodafone or its subcontractors and agents (and obtain consents from third parties to allow) to:
 - (A) access the Buyer Sites, and any Buyer Equipment, Fixed Equipment or Equipment, and third party property located there, as Vodafone reasonably requires to perform its obligations under this Agreement (including for the purposes of installing and uninstalling Equipment (whether in the Buyer Sites or outside) and providing and preparing for the provision of, the Services) and including access outside Working Hours; and
 - (B) ensure that Buyer Sites are safe and have a suitable working environment.
- (e) Emergency Services:
 - (i) General: In the event of a power cut or failure affecting Buyer's fixed line and/or broadband Service, Buyer may not be able to make calls including calls to emergency services.
 - (ii) Buyer obligations: Buyer shall:
 - (A) provide Vodafone with complete and accurate Buyer Site address information; and
 - (B) give Vodafone at least 30 days' written notice of any change to the location of any Fixed Equipment and to any change to the relevant Buyer Site address information



RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector

- (C) Buyer acknowledges that any failure to provide the information required may render emergency services unable to identify User's location.
 - (iii) Calls using the internet: Additionally, where a Service places calls using the internet, Buyer shall:
 - (A) make Users accessing the Service via a soft client aware that Vodafone may be unable to automatically determine their location if they make an emergency services call using the Services; and
 - (B) ensure that such Users provide their location details in the event that they make an emergency services call using the Services. In the event of a power failure, the emergency call placed will be routed over the Network and not through the Service.
 - (f) Unless otherwise agreed and stated in the Buyer's Call-Off Contract, the Buyer will be liable for any additional costs charged to Vodafone by third parties in connection with the provision of the Services. Such charges (often referred to as Excess Construction Charges) are detailed in the Ancillary Services section of this Service Offer. These charges will be notified to the Buyer before any construction works take place and In the event that this results in an increased price from the call off the Buyer has the right to cancel this call off contract in accordance with the terms of this Service Offer and Call off Contract.
 - (g) This Service Offer is subject to survey. In the event that a Site Survey output results in an increased price from the call off the Buyer has the right to cancel this call off contract in accordance with the terms of this Service Offer and Call off Contract.
- 2.3 Tiered Support Services conditions on Buyer
- (a) Buyer shall provide Vodafone with an email address for correspondence and shall be responsible for keeping Vodafone updated of any change.
 - (b) Buyer shall carry out an initial analysis of any Incident reported to its Buyer's Service Desk, to establish whether the Incident should be referred to Vodafone. Buyer shall ensure it provides Vodafone with a key site list of all Buyer Sites that require BMI on or before the Service Commencement Date and shall further ensure that it notifies Vodafone of any updates or amendments to the key site list during the relevant Initial Period. The Buyer is required to ensure that the first key site list and any updates or amendments to the key site list are notified by email to the appointed service manager at Vodafone.
 - (c) Service Desk: Buyer's Service Desk is the service desk provided by Buyer that will be the initial point of contact between Vodafone and Buyer, in relation to the Tiered Support Services.
 - (d) Buyer shall nominate, and notify Vodafone of, one or more points of contact that shall be the primary management interface between Buyer and Vodafone and who shall have the authority contractually to bind Buyer for the purpose of enabling Vodafone to deliver the Tiered Support Services.
- 2.4 Local Area Network with Wi-Fi - Conditions on Buyer
- The Buyer shall:
- (a) Purchase LAN hardware via the Buyer's account manager.
 - (b) Provide Vodafone with a contact email address to be used for account administration purposes, including by a Vodafone shared services team based in India. The email address can be either a personal email address or a generic email address. If the Buyer provides a general email address, this must be a uniquely identifiable email address attributable to an individual user (for example LANadministrator1@Buyer.com, LANadministrator2@Buyer.com, etc.).
 - (c) Provide details to facilitate the delivery, provisioning and billing of the services requested by Vodafone at the time of ordering.
 - (d) Notify Vodafone in advance If Buyer moves Supported Equipment to a new Buyer Site and requires continuance of the Services. Vodafone is under no obligation to provide the Services at the new Buyer Site but will use reasonable endeavours to comply with Buyer's request subject to agreement of Charges which may apply in relation the change of location.



RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector

- (e) Agree, except where Vodafone and Buyer have entered into a separate agreement for the supply of structured cabling:
 - (i) structured cabling is not covered under the Services;
 - (ii) Buyer is responsible for the structured cabling;
 - (iii) any faults resulting from a failure in Buyer's structured cabling will be referred back to Buyer; and
 - (iv) moves and changes of structured cabling are not included as part of the Service.
- (f) Acknowledge and agree Vodafone may use reasonable endeavours to support Equipment that is 'end of life' provided that no Service Credits will apply in relation to such support.
 - (i) The Buyer shall not (and shall ensure that Users shall not) connect or seek to connect the Services to the PSTN otherwise than in accordance with Applicable Law.
 - (ii) Agree that where required by Applicable Law, the Services may be provided in a given country by a Third Party Provider which has the necessary authority to provide the Services. Buyer shall be aware that in certain geographic locations, Vodafone will provide the Services through the use of a local Third Party Provider.
- (g) Acknowledge and agree Vodafone will use reasonable endeavours to maintain an up to date inventory of the Supported Equipment in Vodafone's inventory system. This will include:
 - (i) device name;
 - (ii) serial number;
 - (iii) modules installed; and
 - (iv) applicable service level.
- (h) Managed Wi-Fi Service – Conditions on Buyer
 - (i) Buyer shall prepare "User Terms" governing use of the Services by Users and shall ensure that all Users accept the User Terms before accessing and using the Services and comply with the User Terms in relation to such use. The User Terms shall at a minimum contain provisions which:
 - (A) protect the intellectual property rights relating to the Services;
 - (B) prohibit misuse of the Services;
 - (C) oblige Users to keep secret and not disclose passwords and other security information used to access the Service;
 - (D) obtain the express consent of Users in relation to the processing of data including where applicable Personal Data for the purposes specified in this Service Offer and
 - (E) include appropriate disclaimers and limitations of liability in relation to the Services including a disclaimer, to the extent permitted by applicable law, of implied terms relating to the Services.
 - (ii) Buyer is permitted to resell access to the Service infrastructure within its directly owned and operated network but is not permitted to resell the Service as a complete solution.
 - (iii) Buyer acknowledges and agrees that Third Party Provider(s) named in the Third Party Provider User License Terms may collect and process information in real time (including access point MAC, probing client MAC, time stamps, Received Signal Strength Indication ("RSSI") and channel utilization (collectively the "Collected Data")) in order to provide Buyer with access to data analytics relating to the Collected Data, for example the identification of returning visitors by their MAC addresses, visit duration established by probe requests, and the use of RSSI information to distinguish passers-by from visitors. Buyer acknowledges that Vodafone is neither data controller nor data processor in relation to Collected Data.
 - (iv) Buyer acknowledges use of Managed Wi-Fi Service shall be subject to Cisco Meraki's end Buyer agreement as updated by Cisco Meraki from time to time and published on Cisco Meraki's website at URL <http://www.cisco.com/go/eula>



RM6116 Network Services 3
Lot 2a - Intra Site Connectivity
Vodafone Local Area Network (including Wi-Fi)
Public Sector

3. Outline Implementation Plan

- 3.1 Vodafone provides the Customer with a comprehensive service, moving the Customer from the Service Commencement Date per the Call-Off Contract to the Customer’s first bill. Vodafone’s outline Implementation Plan is detailed below, and this will be updated to become the draft Implementation Plan once the Order Form has been received by Vodafone:
- (a) With the Customer’s Vodafone account manager, Vodafone agrees on a scope document containing an outline of the changes being implemented under the new Call-Off Contract.
 - (b) With a representative from the Customer’s organization, Vodafone will have a call to discuss next steps.
 - (c) Following the call, and Vodafone’s analysis of the Customer’s existing services Vodafone will formulate a draft Implementation Plan for the Customer’s agreement.
 - (d) Vodafone and the Customer will agree a target migration or implementation date and manage all the intermediate activities supporting it.

4. Exit Management Plan

- 4.1 Whether the Buyer would like to cease or move their Services to a new provider entirely, Vodafone’s Exit Management plan is outlined below;
- (a) The Buyer will notify Vodafone of its plan to cease or migrate away from any Service within the Initial Period agreed within the Call Off-Contract.
 - (b) Vodafone will extract a contract end date report, which will detail the current account set up, and any applicable termination fees that will apply to the Buyers final invoice.
 - (c) Upon formal request from the Buyer, Vodafone, where applicable, will generate relevant authorisation/ decommissioning codes in accordance with applicable Law and regulation.
 - (d) The Buyer will manage their relationship and migration plan with their new supplier and, if applicable, share any relevant data provided by Vodafone to their new supplier.
 - (e) If applicable Buyer shall return to Vodafone or destroy the SIMs, as requested by Vodafone.

5. Service Level Agreement

- For the purposes of this Service Offer:
 - (a) The provisions of this Service Level Agreement are compliant with the Service Maintenance Level 1 as set out in Schedule 14 of the Call-Off Terms.
- Vodafone Tiered Support Service Model
 - (b) In addition to the Service Level Agreement in Service Maintenance Level 1 as set out in Schedule 14 of the Call-Off Terms the Buyer will also benefit from the following additional Tiered Support Service Model (“TSSM”) as part of the Service,
 - (i) Service Request Fulfilment Support Services:
 - (A) Response and Acknowledgement

Deliverable	Contact Method	SLT
Vodafone Initial Response	Email	Near Instant



RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector

(ii) Incident Management Support Services:

(A) Incident Management Response and Acknowledgement:

Deliverable	Contact Method	SLT
Vodafone will provide the means to report an Incident and provide an Initial Response by the same means.	Telephone	90% of calls answered <20 seconds

(B) Incident Management Diagnosis:

Deliverable	Contact Method	SLT
Following an Initial Response and as part of initial diagnosis, Vodafone will: (a) determine the Infrastructure Service or Supported System on which the incident has occurred; and (b) determine the perceived impact and urgency of the incident including assessment against the criteria for a Major Incident Vodafone will route the Incident Record to the appropriate support function for expert diagnosis and subsequent management.	Telephone	<30 minutes
Vodafone will contact the party raising the incident to confirm Resolution and closure.	Telephone	<24 hours from Resolution

(iii) Financial Management (Billing) Support Services:

(A) Billing Queries:

Deliverable	Contact Method	SLT
Vodafone will provide the means to raise billing queries and provide an Initial Response via email	Email	Near Instant
Vodafone will ensure that all billing queries received via email are Acknowledged	Email	<24 hours
Vodafone will provide the means to raise billing queries and provide an Initial Response via telephone	Telephone	90% <20 seconds
Vodafone will ensure that all billing queries received via telephone are Acknowledged.	Telephone	Near Instant

(iv) Operational Change Management Support Services

- (A) A Vodafone-designated "Change Manager" will be responsible for changes and the change management process established by Vodafone from time to time. The Change Manager may be from Vodafone, Buyer or a third party, dependent upon where Vodafone (acting reasonably) determines that responsibility for change governance resides.

(B) Notification of Planned and Essential Operational Changes:

Deliverable	Contact Method	SLT
Vodafone will provide notification of a Planned Outage	Email	10 Working Days
Vodafone will notify Buyer in advance, where reasonably possible, of the scheduling of an Essential Outage	Email	>48 hours



RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector

(v) Service Request Catalogues

- (A) Vodafone may make one or more "Service Request Catalogues" available to Buyer through its online portal at OnePortal ("Portal"). A URL for the Portal will be provided to the Buyer via the support handbook. Service Request Catalogues contain information about the Tiered Support Services and Service Requests, including those Service Requests that will be self-served by the Buyer and those that will be serviced by Vodafone, broken down by Service.
- (B) Any Service Request Catalogue information made available to Buyer is provided for guidance only; it is not binding on Vodafone and does not form part of this Agreement.
- (C) Vodafone may change the information contained in the Service Request Catalogue at its discretion, via a catalogue update, provided that the changes do not materially affect the nature of the Tiered Support Services delivered to Buyer.

6. Optional Schedules

This Service Offer assumes that the Buyer is not electing to take any of the following Optional Schedules

- 6.1 Call-Off Schedule 4 of the Call-Off Contract shall not apply.
- 6.2 Call-Off Schedule 6 of the Call-Off Contract shall not apply.
- 6.3 Call-Off Schedule 7 of the Call-Off Contract shall not apply.
- 6.4 Call-Off Schedule 10 of the Call-Off Contract shall not apply.
- 6.5 Call-Off Schedule 11 of the Call-Off Contract shall not apply.
- 6.6 Call-Off Schedule 13 of the Call-Off Contract shall not apply.
- 6.7 Call-Off Schedule 15 of the Call-Off Contract shall not apply.
- 6.8 Call-Off Schedule 16 of the Call-Off Contract shall not apply.
- 6.9 Call-Off Schedule 17 of the Call-Off Contract shall not apply.
- 6.10 Call-Off Schedule 18 of the Call-Off Contract shall not apply.
- 6.11 Call-Off Schedule 22 of the Call-Off Contract shall not apply.
- 6.12 Call-Off Schedule 23 of the Call-Off Contract shall not apply.
- 6.13 Call-Off Schedule 24 of the Call-Off Contract shall not apply.
- 6.14 Call-Off Schedule 25 of the Call-Off Contract shall not apply.
- 6.15 Joint Schedule 6 of the Call-Off Contract shall not apply.
- 6.16 Joint Schedule 7 of the Call-Off Contract shall not apply.
- 6.17 Joint Schedule 8 of the Call-Off Contract shall not apply.
- 6.18 Joint Schedule 9 of the Call-Off Contract shall not apply.

Should the Buyer wish to take any of the above schedules, then these may be subject to additional charges. Please contact your Vodafone account manager, or frameworks_team@vodafone.com who will clarify your requirements, and where needed publish a new Service Offer containing the selected Optional Schedules.



RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector

7. Mandatory Schedules

- 7.1 In accordance with the Supplier's obligations under any Call-Off Contract, Vodafone has developed and will maintain the following reports and plans, which are available to view, download, print or save, on Vodafone's Public Sector Portal. By entering into a Call-Off Contract, the Buyer confirms that it accepts the following reports and plans as is, with no alteration:
- (a) Call-Off Schedule 1 (Transparency Reports) - Transparency Report in accordance with clause 1, of Call-Off Schedule 1.
 - (b) Call-Off Schedule 8 (Business Continuity and Disaster Recovery) – Business Continuity and Disaster recovery Plan in accordance with Clause 1, of Call-Off Schedule 8.
 - (c) Call-Off Schedule 9 (Security) -Security Management Plan in accordance with Clause 4, of Call-Off Schedule 9.
- The Security Management Plan for any Deliverables purchased under this Service Offer shall be the Supplier's Security Management Plan published on Vodafone's Public Sector Portal. By entering into a Call-Off Contract the Buyer acknowledges and agrees:
- (i) The Supplier has prepared and delivered the Security Management Plan (published as set out above) to the Buyer; and
 - (ii) The Buyer has approved the Security Management Plan, in accordance with paragraphs 4.3.1 and 4.3.2 of Call-Off Schedule 9 (Security) Part A: Short Form Security Requirements.

8. Service Description and Price Card

Vodafone's wired and wireless Local Area Network (LAN) solution give users secure and reliable access to business systems and resources from any device.

A local area network (LAN) is a network that interconnects computers within a limited area such as a home, office building or warehouse. A LAN will interconnect to a Wide Area Network (WAN) or the internet by an external fixed communications line.

Ethernet and Wi-Fi are the two most common transmission technologies in use for local area networks.

Vodafone's technology partner of choice is Cisco (including Meraki), who are recognised as a market leader in wired and wireless LAN technology.

Under this Service Offer, Buyers may take the hardware devices that form the LAN and in addition may take one of the incremental Service Wraps.

8.1 Primary Services

The Services shall be based on the delivery of solutions from a single vendor, Cisco Systems Limited, and consist of:

- LAN Design and Build
- Maintained LAN (including Wi-Fi) - detailed as Maintained in the price card below.
- Monitored ("Monitoring") LAN (including Wi-Fi) – detailed as Monitoring in the price card below.
- Managed ("Management") LAN (including Wi-Fi) - detailed as Management in the price card below.

The types of equipment supported shall include but not limited to:

- Wireless access points
- Meraki access points
- Meraki or Cisco switches



RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector

Each device requires a licence to operate. In the case of the security appliance, there are two types. If the Buyer requires Antivirus, Anti Phishing or Content filtering then the Buyer will need to select the Advanced Security & Support Licence, if not then select the Enterprise & Support Licence.

LAN Design and Build

The LAN Design and Build Service shall include professional services to provide local connectivity services at a single site, multiple sites in the same locale, campus sites, and metropolitan area sites, enabling an end user/end user device to connect and consume a locally hosted service.

Maintained LAN

The Maintained LAN Service shall provide remote and onsite support for LAN and WLAN equipment, including fault reporting and service restoration activities. The Service can be applied at a single site, multiple sites in the same locale, campus sites, and metropolitan area sites for the ongoing support of LAN and Wireless LAN equipment that enables an end user/end user device to connect and consume a locally hosted service.

The Buyer shall have the option for the Maintained LAN Service to provide support cover for specific items of equipment in their infrastructure or for the entire LAN/WLAN infrastructure. Bronze Maintenance is offered as part of the RM6116 Standard Service Offer.

Service level	Restore SLA
Gold	5hr
Silver	8hr
Bronze	24hr

Monitored LAN

The Monitored LAN Service shall provide 24x7 remote monitoring of LAN and WLAN equipment. The Service can be provided at a single site, multiple sites in the same locale, campus sites, and metropolitan area sites. The Buyer shall have the option for the Service to provide cover for specific items of equipment in their infrastructure or for the entire LAN/WLAN infrastructure.

This Service is only available when taken in conjunction with the Maintained LAN Service.

The Service shall continually monitor designated equipment on the Buyers LAN/WLAN infrastructure to identify service defects, incidents, and alarms and shall initiate a fault response, notifying the appropriate Vodafone resolver group and the Buyer's nominated representative of such an occurrence. Faults and incidents shall be progressed for resolution by the Vodafone Help Desk to the agreed Service Maintenance Levels.

Managed LAN

The Managed LAN Service provides 24x7 management of LAN and WLAN equipment. The Service can be provided at a single site, multiple sites in the same locale, campus sites and metropolitan area sites. The Buyer shall have the option for the Service to provide cover for specific items of equipment in their infrastructure or for the entire LAN/WLAN infrastructure.

This Service is only available when taken in conjunction with the Maintained and Monitored LAN Services.

The Managed LAN Service provides 'day-to-day' support for such activities as Moves, Adds and Changes (MACs). Vodafone shall take responsibility for the overall health of the network, including equipment software revision levels, change and configuration management and capacity planning.



RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector

Managed wi-fi:

Vodafone provides the Managed Wi-Fi Service in conjunction with Cisco Meraki, LLC (a member of the Cisco Systems, Inc. group of companies) ("Cisco Meraki"). The Managed Wi-Fi Service provides Customer with wireless access points within Customer's premises and includes (i) 'out of band cloud management' where user traffic is separated from wireless access management traffic, (ii) a web-based dashboard giving Customer visibility into its network, devices and applications; (iii) access to location based analytics information and an API that allows analytics information to be shared with Customer systems.

The Managed Wi-Fi Service is delivered by Cisco Meraki will provide certain components of the Service to Buyer as follows:

- (a) Proactive Monitoring via the Cisco Meraki Portal/Dashboard.
 - (i) To deliver monitored and managed service for Managed Wi-Fi, Vodafone will use the Cisco Meraki Dashboard (Dashboard) to monitor the status of devices, manage deployment of devices and set granular user, device and application policies. This system will also be used to diagnose the cause of incidents and to make changes as requested by Buyer.
 - (ii) Vodafone will provide Buyer with access to the dashboard which allows Buyer to monitor its devices over the Internet and provides Buyer with organization-wide reporting information including license status, device counts and network health, including whether devices are alerting or offline.
- (b) Access to the Dashboard.
 - (i) Access to the Dashboard is dependent on the services that Buyer purchases.
 - (ii) Buyers who purchase devices without support or purchase the Monitored or Maintained variant of the Wi-Fi Service will receive full access (Read/Write) to the Portal.
 - (iii) Buyers who purchase devices with the Managed variant of the Wi-Fi Service will be granted limited access to the dashboard. This will exclude the capability for Buyer to configure the devices under support.

Pricing

Pricing for the Service consists of both one-off and annual recurring charges. The total charges for the Service are dependent on a number of factors specific to Buyer requirements as set out in the Order Form.

- **One-Off Charges** consist of the Charges for equipment purchased (including licences), installation and survey services, and any subsequent licence charges applicable (in the event of a licence expiry).
- **Annual Recurring charges** consist of the sum of the Service Wraps selected from the options below:

Maintained:	The Maintained pricing is based on the Buyer's physical estate, including the chassis, modules, interfaces and software.
Monitored:	The Monitored pricing is based on a flat rate per device.
Managed:	The Managed pricing is based on a flat rate per device.

- All prices are quoted in £GBP and exclusive of sales taxes.
- Pricing is for the supported products as detailed in the Price Card.



RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector

Pricing for 12 Month Contract

Meraki LAN and Wi-Fi Licences

Part Number	Part Description	Quantity
LIC-ENT-1YR	Meraki MR Enterprise License, 1YR	49
LIC-MS225-24P-1YR	Meraki MS225-24P Enterprise License and Support, 1YR	10
LIC-MX65-SEC-1YR	EOS Meraki MX65 Advanced Security License and Support, 1YR	2
LIC-MX68-SEC-1YR	Meraki MX68 Advanced Security License and Support, 1YR	1
LIC-MX250-SEC-1YR	Meraki MX250 Advanced Security License and Support, 1YR	1

LAN Kit

Part Number	Part Description	Quantity
C9200-48T-E	C9200-48T-E	6
C9200L-24P-4X-E	C9200L-24P-4X-E	2
C9200L-48T-4X-E	C9200L-48T-4X-E	6
C9300-24T-A	C9300-24T-A	2
C9300-48T-A	C9300-48T-A	2
WS-C2960+24PC-L	WS-C2960+24PC-L	2
WS-C2960+48PST-L	WS-C2960+48PST-L	6
WS-C2960X-48FPD-L	WS-C2960X-48FPD-L	9
WS-C3650-24TS-E	WS-C3650-24TS-E	4
WS-C3850-24T-E	WS-C3850-24T-E	2

Managed LAN

Type	One off Charges - NRC	Monthly Charge (£) MRC	Annual Charge (£) ARC
LAN Maintenance	£0	£1,834.51	£22,014.15
LAN Monitoring	£0	£119.00	£1,428.00
LAN Management	£0	£807.50	£9,690.00
Totals ex VAT	£0	£2,761.01	£33,132.15



RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector

Meraki Wi-Fi

Type	One off Charges - NRC	Monthly Charge (£) MRC	Annual Charge (£) ARC
Wi-Fi Maintenance	£10,493.00	£110.87	£1,330.46
Totals ex VAT	£10,493	£110.87	£1,330.46

ISE Maintenance

Type	One off Charges - NRC	Monthly Charge (£) MRC	Annual Charge (£) ARC
ISE Maintenance	£0	£1,212.05	£14,544.56
Totals ex VAT	£0	£1,212.05	£14,544.56

8.2 Technology, Equipment and Solutions

(a) Ancillary Charges associated with services provided by a third party /OLO

- (i) Unless otherwise agreed and stated in the Buyer's Call-Off Contract, the Buyer will be liable for any additional costs charged to Vodafone by third parties in connection with the provision of the Services. Such Charges include but are not limited to the following:

Feature	Single Payment Charge £ Exc VAT	Connection Charge £ Exc VAT
Survey Fee/ Planning Charge (Previously included in other charges) This item will only be charged if Excess Construction Charges are accepted by a customer except for Non Standard Lines where the Survey Fee will be charged with every order. It will be included as an item within the excess charges calculation and each resurvey additional to the first survey will increment the cost by a further £332.00	£332.00	
Breaking/Drilling through each external wall	£86.00	
Breaking/Drilling through each internal concrete wall	£149.00	
Breaking/Drilling through each internal non-concrete wall	£25.00	
Provision of each Pole	£669.00	
Provision of a new footway box (Surface area up to 0.5 sqm)	£867.00	
Provision of a new medium size footway box (Surface area between 0.5 sqm and 1 sqm)	£1,695.00	
Provision of a new large size footway box (Surface area greater than 1 sqm)	£3,099.00	
Provision of a new small carriageway box (Surface area up to 1 sqm)	£2,782.00	
Provision of a new medium size carriageway box (Surface area between 1 sqm and 1.25 sqm)	£4,378.00	
Provision of a new large size carriageway box (Surface area greater than 1.25 sqm)	£5,681.00	
Cable (fibre or copper) including any jointing required (per metre)		£9.00
Copper cable supplied for the customer to lay to agreed entry and termination points (per metre). (minimum 20m supply) This charge includes on site termination and jointing work by Openreach to connect and terminate the cable. If the order is for less than 40 metres then a visit charge will apply - Please See Visit Charges for details.		£4.00
Directly buried cable (including any cable and wayleave costs) (per metre)		£25.00
Moleploughing cable or fibre in subduct (includes any cable and wayleave costs) (per metre)		£13.00

RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector



Blown Fibre (per metre)		£3.00
Blown Fibre Tubing in Duct (per metre)		£5.00
Fibre Cable (per metre)		£8.00
Internal cabling (including Internal Blown Fibre Tubing) (per metre)		£10.00
New Ductwork - Softsurface (includes wayleave costs) (per metre)		£34.00
New Ductwork - Footway (includes wayleave costs) (per metre)		£78.00
New Ductwork - Carriageway (includes wayleave costs) (per metre)		£148.00
Trunking and traywork within end-user's curtilage (per metre)		£14.00
Overblow Services (per 100 metres)		£427.00

(b) Site Visits By Vodafone

- (i) Additional site visits requested by the Buyer or abortive site visits will be charged as per the following table;

Ancillary Charge per visit	Description	Working Hours	Out of Normal Working Hours A (any time outside of normal Working Hours on Monday to Friday and including any time on Saturday but excluding any time within Out of Normal Working Hours B)	Out of Normal Working Hours B (any time on a Sunday or Public Holiday in the UK)
Site Visit	Buyer Site Visit required or requested (a Site Visit not identified in the Call-Off Contract)	£350	£500	£650
Aborted Site Visit†	Vodafone's engineer Site Visit for an appointment but cannot gain access to do the work required or the site has not been appropriately prepared as per Vodafone instructions	£350	£500	£650
Site Survey	Additional Site Survey	£500	£700	£900
Extended Site Visit	Should the engineer need to extend the period on-site for any Buyer related reason additional charges will be incurred e.g. Access delays, non- adherence to Vodafone instructions	£58/hr or part thereof	£85/hr or part thereof	£106/hr or part thereof
Buyer site visit Fault/Incident outside of Vodafone domain†	Buyer Site Visit to investigate a reported Fault/Incident, which transpires to be outside the domain of the services provided by Vodafone. (e.g. services provided by the Buyer or its Third Party Providers).	£350 for the first 3hrs + £58/hr or part thereof	£500 for the first 3hrs + £85/hr or part thereof	£650 for the first 3hrs + £106/hr or part thereof
Cancelled Site Visit	Buyer caused cancellation of engineering Site Visit Note: No Charge if cancelled more than 48 hours before the scheduled appointment	Within 24hrs of Site Visit = full aborted Site Visit charge Between 24 and 48hrs of Site Visit = 50% of aborted Site Visit charge		

(c) Professional Services

Vodafone a range of professional services including technical consultancy, project management and on-site service management.

Charges	
	Maximum daily rates excluding expenses
Consultants	
Junior Consultant	£ 690
Consultant	£ 720
Senior Consultant	£ 850
Principal Consultant	£ 850



RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector

Partner/ Director	£	1,000
Contractors / IT Specialists		
Senior Analyst/ Team Leader	£	570
Systems Analyst & Designers	£	570
Analyst/ Programmers	£	570
Application Programmers	£	570
System Programmers	£	570
Database Administrators	£	570
Network Administrators	£	430
Capacity Planners	£	570
Configuration Managers	£	570
IT Trainers	£	570
Documentation Specialists	£	380
Project Administrators	£	510

9. Key Sub-Contractors

- Cisco Systems Limited
 - 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA
 - 02558939
- Maintel Limited
 - 95 Rivers Apartment, Cannon Road, London, N17 8FE
 - 03034803

10. Definitions

The following definitions are applicable to this Service Offer:

Acknowledge	a confirmation given to Buyer that a particular request or Incident raised is valid and the provision to Buyer of a unique reference for it. "Acknowledge" shall be construed accordingly.
Agreement	Means the Call-Off Contract, Standard Service Offer and any other applicable document required for the purchase of the Service.
Applicable Law	law, regulation, binding code of practice, rule or requirement of any relevant government or governmental agency, professional or regulatory authority, sanctions (economic trade and financial sanctions laws, regulations, embargoes or restrictive measures administered), trade or export control laws each as relevant to (i) Vodafone in the provision of the Services and/or (ii) Buyer in the receipt of the Services or the carrying out of its business.
AUP	Vodafone's acceptable use policy available on request.
Available Services	The Services available from particular Helpdesks.
Buyer's Service Desk	is the service desk provided by Buyer which will be the initial point of contact between Vodafone and Buyer.
Buyer Site	as the context permits a Buyer's premises (either owned by Buyer or a third party) which Vodafone needs to access in order to deliver or install Equipment and/or to provide the Services or the location where the Services are to be provided, as set out in the Call-Off Contract.
BPE (Buyer premises equipment)	Fixed Equipment on Buyer Site.
BMI	a "Buyer major incident", being the highest category of Impact for an Incident resulting in significant disruption to the business of Buyer.



RM6116 Network Services 3

Lot 2a - Intra Site Connectivity

Vodafone Local Area Network (including Wi-Fi)

Public Sector

Buyer	Where used in this Service Offer or Call-Off Contract means the Buyer
Buyer Equipment	hardware, Software or any other tangible material not supplied by Vodafone that is used with or to access the Service. Any Equipment Buyer purchases from Vodafone shall be considered to be Buyer Equipment once title has passed to the Buyer.
Call Abandonment	Calls made by the Buyer but which the Buyer abandons after waiting for a response for 15 seconds or more.
Contact Number(s)	the telephone numbers required to contact the Helpdesks.
Buyer Services Helpdesk	the call centre operated by Vodafone to provide support services to the Buyer.
End Of Life	where Vodafone or a manufacturer of Equipment declares that the type of Equipment is end-of-life (or otherwise stops marketing, selling or supporting it).
Equipment	hardware, Vodafone Software, and any other tangible equipment (other than SIMs) supplied by, or on behalf of, Vodafone to Buyer for use in receiving the Services. Equipment excludes Buyer Equipment.
Essential Outage	an Outage that is not a Planned Outage including, but not limited to, Outages caused by a force majeure event or an act or omission of any third party which is beyond Vodafone's reasonable control.
Fixed Equipment	hardware, Vodafone Software, BPE and any other tangible equipment (other than SIMs and mobility equipment) supplied by or on behalf of, Vodafone to Buyer for use in receiving the Services.
GSM Gateway	any equipment containing a SIM card which enables the routing of calls from fixed apparatus to mobile equipment by establishing a mobile to mobile call.
Helpdesk(s)	the Buyer Services Helpdesk or Buyer Management Centre.
Incident	an unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected Service is also an Incident.
Incident Record	a record containing the details and lifecycle of an Incident.
Infrastructure Services	an IT service that is not directly used by Buyer's business, but is required for the provision of other IT services (for example either a Functional Service, connectivity service, hosting service or any combination thereof).
Initial Response	a first response from Vodafone to an individual raising a request or Incident, such as answering the telephone or replying to an email.
Operating Hours	the hours during which the Helpdesks are available.
Network	the communications network together with the equipment and premises that are connected to such network and which are used by Vodafone to perform the Services.
Mandatory Accompanying Services	any mandatory accompanying services specified in the Service Specific Terms relating to a Service.
Planned Outage	the scheduled unavailability of an Infrastructure Service.
Resolution	the exercise by Vodafone of its reasonable endeavours to repair the root cause of an Incident or Problem, or to implement a workaround.
Services	the Vodafone product(s) detailed in this Service Offer.
Service Commencement Date	the date of completion of Vodafone's testing when the Service is ready for use.
Supplier	Where used in this Service Offer or Call-Off Contract means Vodafone
Service Request	a request from a user for information, or advice, or for a Standard Change or for access to an IT service made in accordance with the requirements of the relevant Service Request Catalogue.
Site Survey	a survey of a Buyer's Site to assess whether (in Vodafone's opinion) the existing infrastructure is sufficient for providing the Services and detailing what the Buyer needs to do to receive the Service.



RM6116 Network Services 3
Lot 2a - Intra Site Connectivity
Vodafone Local Area Network (including Wi-Fi)
Public Sector

Third Party Provider	a Key Subcontractor or third party contracted by Vodafone or Buyer that provides a Service, or that provides a service that connects to a Service.
User	an individual end user of the Services who is approved by Buyer and who must be a permanent or temporary employee or sub-contractor of Buyer or an Additional Service Recipient unless otherwise specified in this Agreement.
User Details	a username, password, or other access information used by a User to access the Service and/or Equipment.
Vodafone Software	any Software supplied by Vodafone or its licensors to Buyer (including Software embedded in any Equipment).
Vodafone	Vodafone Limited, registered number 01471587, and registered office Vodafone House, The Connection, Newbury, Berkshire RG14 2FN.
Working Days	Monday to Friday inclusive, other than public holidays in the UK.
Working Hours	the hours between 8.00am and 6.00pm on each Working Day.