



G-Cloud 14 Call-Off Contract

This Call-Off Contract for the G-Cloud 14 Framework Agreement (RM1557.14) includes:

G-Cloud 14 Call-Off Contract

[Part A: Order Form](#)

[Part B: Terms and conditions](#)

[Schedule 1: Services](#)

[Schedule 2: Call-Off Contract charges](#)

[Schedule 3: Collaboration agreement](#)

[Schedule 4: Alternative clause](#)

[Schedule 5: Guarantee](#)

[Schedule 6: Glossary and interpretations](#)

[Schedule 7: UK GDPR Information](#)

[Annex 1: Processing Personal Data](#)

[Annex 2: Joint Controller Agreement](#)

[Schedule 8: Corporate Resolution Planning](#)

[Schedule 9 : Variation Form](#)

[Schedule 10: Security](#)

Part A: Order Form

Buyers must use this template order form as the basis for all Call-Off Contracts and must refrain from accepting a Supplier's prepopulated version unless it has been carefully checked against template drafting.

Platform service ID number	274546631612186
Call-Off Contract reference	P3389
Call-Off Contract title	UKSV Network Infrastructure Review
Call-Off Contract description	UKSV (part of the Cabinet office) are seeking an organisation who specialise in Infrastructure/network reviews. The supplier will provide specialist in-depth understanding of the services that UKSV use and the existing connectivity from UKSV in order to support the activity to potentially become an Arm's length body.
Start date	01 April 2025
Expiry date	30 September 2025
Call-Off Contract value	£99,850
Charging method	Monthly Payments in arrears by BACS
Purchase order number	TBC post contract signature

This Order Form is issued under the G-Cloud 14 Framework Agreement (RM1557.14).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Services offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

From the Buyer	Cabinet Office (UKSV) Government Security Function Centre 70 Whitehall London SW1A 2AS
To the Supplier	UBDS IT CONSULTING LTD Level 1 Brockbourne House, 77 Mount Ephraim, Tunbridge Wells, Kent, England, TN4 8BS. tel:0330 111 0066 Company number 04330005

Together the 'Parties'

Principal contact details

For the Buyer:

Title: [REDACTED]

Name: [REDACTED]

Email: [REDACTED]

For the Supplier:

Title: [REDACTED]

Name: [REDACTED]

Email: [REDACTED]


Phone: [REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 1 st April 2025 and is valid for six (6) months.
Ending (termination)	<p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums (as per clause 18.6).</p> <p>The notice period for the Buyer is a maximum of 30 days from the date of written notice for Ending without cause (as per clause 18.1).</p>
Extension period	Not Used.

Buyer contractual details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

G-Cloud Lot	<p>This Call-Off Contract is for the provision of Services Under:</p> <ul style="list-style-type: none">• Lot 3: Cloud support
G-Cloud Services required	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined in the following separate documentation.</p> <ul style="list-style-type: none">• Schedule 1A Service Definition Document• Schedule 1B UKSV Network Infrastructure Review SOR.• Schedule 1C Pricing document
Additional Services	Not Used
Location	<p>The Services will be delivered mainly virtually via Microsoft teams, google meet. Occasional travel may be required to one of the UKSV offices based in York, Glasgow or Manchester.</p>
Quality Standards	<p>The quality standards required for this Call-Off Contract are within Schedule 1A Service Definition Document, Schedule 1B UKSV Network Infrastructure Review SOR and Schedule 1C Pricing document</p>
Technical Standards:	NOT USED
Service level agreement:	NOT USED
Onboarding	

Offboarding	NOT USED
Collaboration agreement	NOT USED
Limit on Parties' liability	<p>Defaults by either party resulting in direct loss or damage to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed £100,000 per year.</p> <p>The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation of or damage to any Buyer Data will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>The annual total liability of the Supplier for all other Defaults will not exceed the greater of 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>
Buyer's responsibilities	<p>The Buyer is responsible for access and availability of key Stakeholders, including external stakeholders and third party suppliers.</p> <ul style="list-style-type: none"> • The Buyer will assign a stakeholder who is responsible for agreeing priorities and who will act as a lead point of contact • The Buyer provides meeting rooms to hold face-to-face meetings as required. • The Buyer to sponsor and, where necessary, expedite security clearances required by Supplier team.

Buyer's equipment	Buyer to provide secure laptops if required for access to network configuration.
--------------------------	--

Supplier's information

Subcontractors or partners	NOT USED
-----------------------------------	----------

Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

Payment method	The payment method for this Call-Off Contract is BACS
Payment profile	The expected payment profile for this Call-Off Contract is monthly in arrears].
Invoice details	The Supplier will issue electronic invoices once a month end timesheet has been signed off by the Buyer. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.

Who and where to send invoices to	Invoices will be sent to [REDACTED] [REDACTED]		
Invoice information required	All invoices must include the full address, have a valid Purchase Order (PO) number which will be provided by the Buyer to [REDACTED] [REDACTED] Invoices must include a full breakdown of charges applied in the preceding month. All invoices must be in PDF format.		
Invoice frequency	Invoice will be sent to the Buyer monthly in arrears.		
Call-Off Contract value	The total value of this Call-Off Contract is £99,850		
Call-Off Contract charges	<p>The monthly breakdown/profile of the Charges estimated below:</p> <div style="background-color: black; height: 200px; width: 100%;"></div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 80%;">Total Excl. VAT</td> <td style="width: 20%; text-align: right;">£99,850</td> </tr> </table>	Total Excl. VAT	£99,850
Total Excl. VAT	£99,850		

Additional Buyer terms

Performance of the Service	<p>This Call-Off Contract will include 2 phases, Phase 1 initial engagement and phase 2 reporting outcomes (the detail of which is included in Schedule 1B UKSV Network Infrastructure Review SOR. The work within each phase is delivered on a T & M basis with monthly billing.</p> <p>The phases are shown below:</p> <table><tr><th>Milestone/ Deliverable</th><th>Description</th><th>Timeframe or Delivery Date</th></tr><tr><td>Phase 1 (Initial Engagement)</td><td>Discovery engagement (external and internal stakeholders)</td><td>Within three months of contract award</td></tr><tr><td>Phase 2 (Reporting outputs)</td><td>Reporting outputs including roadmap</td><td>Within six months of Contract Award</td></tr></table>	Milestone/ Deliverable	Description	Timeframe or Delivery Date	Phase 1 (Initial Engagement)	Discovery engagement (external and internal stakeholders)	Within three months of contract award	Phase 2 (Reporting outputs)	Reporting outputs including roadmap	Within six months of Contract Award
Milestone/ Deliverable	Description	Timeframe or Delivery Date								
Phase 1 (Initial Engagement)	Discovery engagement (external and internal stakeholders)	Within three months of contract award								
Phase 2 (Reporting outputs)	Reporting outputs including roadmap	Within six months of Contract Award								
Guarantee	NOT USED									
Warranties, representations	Incorporated Framework Agreement clause 2.3.									
Supplemental requirements in addition to the Call-Off terms	NOT USED									

Alternative clauses	NOT USED
Buyer specific amendments to/refinements of the Call-Off Contract terms	NOT USED
Personal Data and Data Subjects	Annex 1 of Schedule 7 is being used:
Intellectual Property	NOT USED
Social Value	<p>Suppliers delivering this contract should be familiar with Procurement Policy Note (PPN) 6/20 – Taking Account of Social Value in the Award of Central Government Contracts and where appropriate consider additional benefits that can delivered PPN 06/20 guidance documents can be found at:</p> <p>https://www.gov.uk/government/publications/procurement-policy-note-0620-taking-account-of-social-value-in-the-award-of-central-government-contracts .</p> <p>Suppliers fulfilling this contract will be expected to complete a 'Social Value for Commercial Success' - an e-learning course accessed through the Government Commercial College that can be found via the 'Social Value Mandatory eLearning' link. It takes less than one hour to complete and will help you to better understand what social value is, why it is important and how to implement it. It is expected that the successful supplier will complete this course at no additional cost to the Buyer</p>

Performance Indicators	NOT USED
-------------------------------	----------

1. Formation of contract

1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.





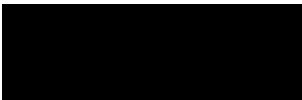
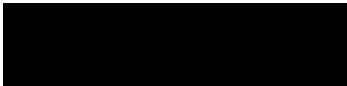
1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.

1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.

1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clauses 8.3 to 8.6 inclusive of the Framework Agreement.

2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.14.

Signed	UBDS IT CONSULTING LTD	Buyer
Name		
Title		
Signature		
Date	05/03/2025	18/03/2025

2.2 The Buyer provided an Order Form for Services to the Supplier.

Buyer Benefits

For each Call-Off Contract please complete a buyer benefits record, by following this link:

Part B: Terms and conditions

1. Call-Off Contract Start date and length

1.1 The Supplier must start providing the Services on the date specified in the Order Form.

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 36 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 36 months

2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses, schedules and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 to 8.6 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)
- 17 (Bribery and corruption)
- 18 (Freedom of Information Act)
- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)
- 24 (Conflicts of interest and ethical walls)
- 25 (Publicity and branding)

- 26 (Equality and diversity)
- 28 (Data protection)
- 30 (Insurance)
- 31 (Severability)
- 32 and 33 (Managing disputes and Mediation)
- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

2.2.1 a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'

2.2.2 a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'

2.2.3 a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 7 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'XX', where 'XX' is the Framework Agreement clause number.

2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

3. Supply of services

3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.

3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form

4. Supplier staff

4.1 The Supplier Staff must:

4.1.1 be appropriately experienced, qualified and trained to supply the Services

4.1.2 apply all due skill, care and diligence in faithfully performing those duties

4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer

4.1.4 respond to any enquiries about the Services as soon as reasonably possible 4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer

- 4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.
- 4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
- 4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.
- 4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.
- 4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14 digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.
- 4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.
- 4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

- 5.1 Both Parties agree that when entering into a Call-Off Contract they:
- 5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
 - 5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms
 - 5.1.3 have raised all due diligence questions before signing the Call-Off Contract
 - 5.1.4 have entered into the Call-Off Contract relying on their own due diligence

6. Business continuity and disaster recovery

- 6.1 The Supplier will have a clear business continuity and disaster recovery plan in their Service Descriptions.
- 6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.

7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

8. Recovery of sums due and right of set-off

8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

9. Insurance

9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

9.2 The Supplier will ensure that:

9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000

9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit

9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers

9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances

9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

10. Confidentiality

10.1 The Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under incorporated Framework Agreement clause 34. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

11.1 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.

11.2 Neither Party shall have any right to use any of the other Party's names, logos or trademarks on any of its products or services without the other Party's prior written consent.

11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:

11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and

11.3.2 The Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer's written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.

11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

11.5 Subject to the limitation in Clause 24.3, the Buyer shall:

11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:

- (a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
- (b) alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;
- (c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and

11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgement against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer's obligations under this Clause 11.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier's breach of this Contract.

11.6 The Supplier will, on written demand, fully indemnify the Buyer for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:

11.6.1 rights granted to the Buyer under this Call-Off Contract

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

11.7 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

11.7.1 modify the relevant part of the Services without reducing its functionality or performance

11.7.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer

11.7.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.8 Clause 11.6 will not apply if the IPR Claim is from:

11.8.1 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract

11.8.2 other material provided by the Buyer necessary for the Services

11.9 If the Supplier does not comply with this clause 11, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

12.1.1 comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data

12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body

12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

12.2.1 providing the Buyer with full details of the complaint or request

12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions

12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)

12.2.4 providing the Buyer with any information requested by the Data Subject

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

13. Buyer data

13.1 The Supplier must not remove any proprietary notices in the Buyer Data.

13.2 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.

13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.

13.5 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.

13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

13.6.1 the principles in the Security Policy Framework:

<https://www.gov.uk/government/publications/security-policy-framework> and the Government Security - Classification policy:

<https://www.gov.uk/government/publications/government-security-classifications>

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: <https://www.npsa.gov.uk/content/adopt-risk-management-approach> and Protection of Sensitive Information and Assets: <https://www.npsa.gov.uk/sensitive-information-assets>

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance: <https://www.ncsc.gov.uk/collection/risk-management-collection>

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint: <https://www.gov.uk/government/publications/technologycode-of-practice/technology-code-of-practice>

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance: <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>

13.6.6 Buyer requirements in respect of AI ethical standards.

13.7 The Buyer will specify any security requirements for this project in the Order Form.

13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

13.9 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at:

<https://www.gov.uk/government/publications/technologycode-of-practice/technology-code-of-practice>

14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.

15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

16. Security

16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.

16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.

16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.

16.4 Responsibility for costs will be at the:

16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided

16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control

16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.

16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:

<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>

16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

17. Guarantee

17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:

17.1.1 an executed Guarantee in the form at Schedule 5

17.1.2 a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided

18.2.2 Call-Off Contract Charges paid during the notice period are reasonable compensation and cover all the Supplier's avoidable costs or Losses

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied

18.4.2 any fraud

18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so

18.5.2 an Insolvency Event of the other Party happens

18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

19.4.1 any rights, remedies or obligations accrued before its Ending or expiration

19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry

19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)
- 24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability), 24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

19.4.4 Any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires.

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it

19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer

19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer

19.5.4 destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written

confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law

19.5.5 work with the Buyer on any ongoing work

19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

20. Notices

20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.

- Manner of delivery: email
- Deemed time of delivery: 9am on the first Working Day after sending
- Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message

20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from CDDO under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the period on terms that are commercially reasonable and acceptable to the Buyer

21.6.2 there will be no adverse impact on service continuity

21.6.3 there is no vendor lock-in to the Supplier's Service at exit

21.6.4 it enables the Buyer to meet its obligations under the Technology Code of Practice

21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.

21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:

21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier

21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer

21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier

21.8.4 the testing and assurance strategy for exported Buyer Data

21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations

21.8.6 any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

22. Handover to replacement supplier

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control

22.1.2 other information reasonably requested by the Buyer

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

23.1 Neither Party will be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Call-Off Contract (other than a payment of money) to the extent that such delay or failure is a result of a Force Majeure event.

23.2 A Party will promptly (on becoming aware of the same) notify the other Party of a Force Majeure event or potential Force Majeure event which could affect its ability to perform its obligations under this Call-Off Contract.

23.3 Each Party will use all reasonable endeavours to continue to perform its obligations under the Call-Off Contract and to mitigate the effects of Force Majeure. If a Force Majeure event prevents a Party from performing its obligations under the Call-Off Contract for more than 30 consecutive Working Days, the other Party can End the Call-Off Contract with immediate effect by notice in writing.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Supplier's liability:

24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited; and

24.2.2 in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.

24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).

24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause 24.2 will not be taken into consideration.

25. Premises

25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer's premises, the Supplier will:

25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises

25.5.2 comply with Buyer requirements for the conduct of personnel

25.5.3 comply with any health and safety measures implemented by the Buyer

25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

27. The Contracts (Rights of Third Parties) Act 1999

27.1 Except as specified in clause 29.8, a person who is not a Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

28. Environmental requirements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to end it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

29.2.1 the activities they perform

29.2.2 age

29.2.3 start date

29.2.4 place of work

29.2.5 notice period

29.2.6 redundancy payment entitlement

29.2.7 salary, benefits and pension entitlements
29.2.8 employment status
29.2.9 identity of employer
29.2.10 working arrangements
29.2.11 outstanding liabilities
29.2.12 sickness absence
29.2.13 copies of all relevant employment contracts and related documents
29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer.

29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

29.5 The Supplier will cooperate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.

29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:

29.6.1 its failure to comply with the provisions of this clause

29.6.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

29.3 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

29.4 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.

31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:

31.2.1 work proactively and in good faith with each of the Buyer's contractors

31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

32.1 The Buyer can request in writing a change to this Call-Off Contract using the template in Schedule 9 if it isn't a material change to the Framework Agreement or this Call-Off Contract. Once implemented, it is called a Variation.

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request using the template in Schedule 9. This includes any changes in the Supplier's supply chain.

32.3 If either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days' notice to the Supplier.

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7.

Schedules 1A, 1B & 1C: Services

The services which have been agreed are in line with:

- Schedule 1A Service Definition Document;

- Schedule 1B UKSV Network Infrastructure Review SOR (contained in a separate document);
- Schedule 1C Pricing Document

Schedule 2: Call-Off Contract charges

Services shall be delivered in line with Schedule 1C Pricing document. The detailed Charges breakdown for the provision of Services during the Term is in accordance with estimated effort below.

Total Exc VAT			2	£99,850

Schedule 3: Collaboration agreement (NOT USED)

Schedule 4: Alternative clauses NOT USED

Schedule 5 NOT USED.

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform).
Audit	An audit carried out under the incorporated Framework Agreement clauses.
Background IPRs	<p>For each Party, IPRs:</p> <ul style="list-style-type: none"> • owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes • created by the Party independently of this Call-Off Contract, or <p>For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.</p>
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.

Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
-----------------------	---

Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form, set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	<p>Data, Personal Data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none"> • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.

Controller	Takes the meaning given in the UK GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.

Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	(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 Subject	Takes the meaning given in the UK GDPR
Default	<p>Default is any:</p> <ul style="list-style-type: none"> • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract <p>Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a</p>

	Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.

ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-fortax

Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Financial Metrics	<p>The following financial and accounting measures:</p> <ul style="list-style-type: none"> • Dun and Bradstreet score of 50 • Operating Profit Margin of 2% • Net Worth of 0 • Quick Ratio of 0.7
Force Majeure	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans

Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.14 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.

Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that 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 in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.

Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.

Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.

Insolvency event	<p>Can be:</p> <ul style="list-style-type: none"> • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium • a Supplier Trigger Event
-------------------------	---

Intellectual Property Rights or IPR	<p>Intellectual Property Rights are:</p> <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 names, 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</p> <ul style="list-style-type: none"> • (c) all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> • the supplier's own limited company • a service or a personal service company • a partnership <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>
IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	<p>All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or Buyer's possession before the Start date.</p>
-----------------	--

Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgement of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgement, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' Losses ' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement Schedule 6.
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.

New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: “Fair Deal for staff pensions: staff transfer from central government” issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and ‘Parties’ will be interpreted accordingly.
Performance Indicators	The performance information required by the Buyer from the Supplier set out in the Order Form.
Personal Data	Takes the meaning given in the UK GDPR.
Personal Data Breach	Takes the meaning given in the UK GDPR.
Platform	The government marketplace where Services are available for Buyers to buy.

Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK GDPR.
Prohibited act	<p>To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:</p> <ul style="list-style-type: none"> • induce that person to perform improperly a relevant function or activity • reward that person for improper performance of a relevant function or activity • commit any offence: <ul style="list-style-type: none"> ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation 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 such measures adopted by it.

PSN or Public Services Network	The Public Services Network (PSN) is the government's high performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.

Service Data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data and Performance Indicators data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controlscheck-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.

Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.

Supplier staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Trigger Event	The Supplier simultaneously fails to meet three or more Financial Metrics for a period of at least ten Working Days.
Variation	This has the meaning given to it in clause 32 (Variation process).
Variation Impact Assessment	<p>An assessment of the impact of a variation request by the Buyer 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 Call-Off Contract; b) details of the cost of implementing the proposed variation;

	<p>c) details of the ongoing costs required by the proposed variation when implemented, including any increase or decrease in the Charges, any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party;</p> <p>d) a timetable for the implementation, together with any proposals for the testing of the variation; and</p> <p>such other information as the Buyer may reasonably request in (or in response to) the variation request;</p>
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Intentionally Blank

Schedule 7: UK GDPR Information

This schedule reproduces the annexes to the UK GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract and clause and schedule references are to those in the Framework Agreement but references to CCS have been amended

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 Buyer at its absolute discretion.

1.1 The contact details of the Buyer's Data Protection Officer are [REDACTED]

1.2 The contact details of the Supplier's Data Protection Officer are: [REDACTED] Contact details: [REDACTED]

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 and Processor for each Category of Personal Data	<p>The Buyer is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:</p> <p><i>The scope of Personal Data which the purposes and means of the Processing by the Supplier is determined by the Buyer</i></p> <p>The supplier will have access to technology infrastructure, environments and configuration data. Personal data will be limited to contact details (name/email) of support personnel only.</p>
Duration of the Processing	<p>The supplier will have access to network infrastructure during the following period.</p> <p>01/04/2025 – 30/09/2025</p>
Nature and purposes of the Processing	<p>The Buyer will make available relevant network infrastructure data in order for the supplier to carry out the discovery and reporting phases of the contract. The supplier will collect this in order to present to the buyer.</p>

Type of Personal Data	Name & email address only – contact details of stakeholders in order to fulfil the work
Categories of Data Subject	UKSV & Ministry of Defence Staff & third-party suppliers as directed and provided by the Buyer.
International transfers and legal gateway	Access is via client secure laptop and will not be stored by the Supplier.
Plan for return and destruction of the data once the Processing is complete	Access is via client secure laptop and will not be stored by the Supplier.

Annex 2 - Joint Controller Agreement (not used)

Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2 to 15 of Schedule 7 (Where one Party is Controller and the other Party is Processor) and paragraphs 17 to 27 of Schedule 7 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the **[Buyer]**:

(a) is the exclusive point of contact for Data Subjects and is responsible for using all reasonable endeavours to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and

(e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the **[Buyer's]** privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. Undertakings of both Parties

2.1 The Supplier and Buyer each undertake that they shall:

(a) report to the other Party every **[3]** months on:

(i) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law, that it has received in relation to the subject matter of the Framework Agreement during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Framework Agreement or is required by Law) that disclosure or transfer of Personal Data is otherwise considered to be lawful processing of that Personal Data in accordance with Article 6 of the UK GDPR or EU GDPR (as the context requires). For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

(e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

(g) use all reasonable endeavours to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

(i) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and

(iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach 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;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and

(j) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.

(k) where the Personal Data is subject to UK GDPR, not transfer such Personal Data outside of the UK unless the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:

(i) the destination country has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR or DPA 2018 Section 74; or

(ii) the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75) as agreed with the non-transferring Party which could include relevant parties entering into the International Data Transfer Agreement (the “**IDTA**”), or International Data Transfer Agreement Addendum to the European Commission’s SCCs (“the **Addendum**”), as published by the Information Commissioner’s Office from time to time, as well as any additional measures;

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

(iv) the transferring Party 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 non-transferring Party in meeting its obligations); and

(v) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data; and

(l) where the Personal Data is subject to EU GDPR, not transfer such Personal Data outside of the EU unless the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:

(i) the transfer is in accordance with Article 45 of the EU GDPR; or

(ii) the transferring Party has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the non-transferring Party which could include relevant parties entering into Standard Contractual Clauses in the European Commission’s decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time as well as any additional measures;

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

(iv) the transferring Party complies with its obligations under EU GDPR by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and

(v) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

3. Data Protection Breach

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and

(b) all reasonable assistance, including:

(i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(ii) co-operation with the other Party including using such reasonable endeavours as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall use all reasonable endeavours to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

4. Audit

4.1 The Supplier shall permit:

(a) The Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

(b) The Buyer, or a third-party auditor acting under the Buyer's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Framework Agreement, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Buyer may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

(a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Framework Agreement, in accordance with the terms of Article 30 UK GDPR.

6. ICO Guidance

The Parties agree to take account of any non-mandatory guidance issued by the Information Commissioner, any relevant Central Government Body and/or any other regulatory authority. The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the Framework Agreement to ensure that it complies with any guidance issued by the Information Commissioner, any relevant Central Government Body and/or any other regulatory authority.

7. Liabilities for Data Protection Breach

7.1 If financial penalties are imposed by the Information Commissioner on either the Buyer or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

(a) if in the view of the Information Commissioner, the Buyer is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Buyer, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Buyer, then the Buyer shall be responsible for the payment of such Financial Penalties. In this case, the Buyer will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Buyer and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

(b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(c) if no view as to responsibility is expressed by the Information Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the procedure set out in clause 32 of the Framework Agreement (Managing disputes).

7.2 If either the Buyer or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

(a) if the Buyer is responsible for the relevant Personal Data Breach, then the Buyer shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Buyer and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Buyer.

8. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Buyer shall be entitled to terminate the Framework Agreement by issuing a Termination Notice to the Supplier in accordance with Clause 5.1.

9. Sub-Processing

9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Framework Agreement, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Framework Agreement), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

Schedule 8 (Corporate Resolution Planning)

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Schedule 6 (Glossary and interpretations):

"Accounting Reference Date"	means in each year the date to which the Supplier prepares its annual audited financial statements;
"Annual Revenue"	<p>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:</p> <p>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</p> <p>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;</p>

<p>“Appropriate Authority” or “Appropriate Authorities”</p>	<p>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;</p>
<p>“Associates”</p>	<p>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;</p>
<p>"Cabinet Office Markets and Suppliers Team"</p>	<p>means the UK Government's team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function;</p>
<p>“Class 1 Transaction”</p>	<p>has the meaning set out in the listing rules issued by the UK Listing Authority;</p>

“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 Services; (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 Services; (d) a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the London Stock Exchange plc; (e) an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking place in respect of the Supplier or any Parent Undertaking of the Supplier; (f) payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the Net Asset Value of the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any 12 month period;

	<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>
"Corporate Change Event Grace Period"	means a grace period agreed to by the Appropriate Authority for providing CRP Information and/or updates to Business Continuity Plan after a Corporate Change Event;
"Corporate Resolvability Assessment (Structural Review)"	means part of the CRP Information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraph 3 and Annex 2 of this Schedule;

<p>“Critical National Infrastructure” or “CNI”</p>	<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>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>significant impact on the national security, national defence, or the functioning of the UK;</p>
<p>“Critical Service Contract”</p>	<p>means the overall status of the Services provided under the Call-Off Contract as determined by the Buyer and specified in Paragraph 2 of this Schedule;</p>
<p>“CRP Information”</p>	<p>means the corporate resolution planning information, together, the:</p> <p>(a) Exposure Information (Contracts List);</p> <p>(b) Corporate Resolvability Assessment (Structural Review); and</p> <p>(c) Financial Information and Commentary</p>

<p>“Dependent Parent Undertaking”</p>	<p>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 Call-Off Contract, including for the avoidance of doubt the provision of the Services in accordance with the terms of the Call-Off Contract;</p>
<p>“FDE Group”</p> <p>“Financial Distress Event”</p>	<p>means the [Supplier, Subcontractors, [the Guarantor]</p> <p>the credit rating of an FDE Group entity dropping below the applicable Financial Metric;</p> <p>an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;</p> <p>there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity;</p> <p>an FDE Group entity committing a material breach of covenant to its lenders;</p> <p>a Subcontractor notifying CCS or the Buyer that the Supplier has not satisfied any material sums</p>

	<p>properly due under a specified invoice and not subject to a genuine dispute;</p> <p>any of the following:</p> <p>commencement of any litigation against an FDE Group entity with respect to financial indebtedness greater than £5m or obligations under a service contract with a total contract value greater than £5m;</p> <p>non-payment by an FDE Group entity of any financial indebtedness;</p> <p>any financial indebtedness of an FDE Group entity becoming due as a result of an event of default;</p> <p>the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity;</p> <p>or</p> <p>the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity;</p> <p>in each case which the Buyer reasonably believes (or would be likely to reasonably believe) could directly impact on the continued performance and delivery of the Services in accordance with the Call-Off Contract; and</p> <p>any two of the Financial Metrics for the Supplier not being met at the same time.</p>
“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;
“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;
“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

<p>“UK Public Sector / CNI Contract Information”</p>	<p>means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 3 to 5 and Annex 1;</p>
---	--

2. Service Status and Supplier Status

2.1 This Call-Off Contract is not a Critical Service Contract.

2.2 The Supplier shall notify the Buyer and the Cabinet Office Markets and Suppliers Team in writing within 5 Working Days of the Start Date and throughout the Call-Off Contract Term within 120 days after each Accounting Reference Date as to whether or not it is a Public Sector Dependent Supplier. The contact email address for the Markets and Suppliers Team is resolution.planning@cabinetoffice.gov.uk.

2.3 The Buyer and the Supplier recognise that, where specified in the Framework Agreement, CCS shall have the right to enforce the Buyer's rights under this Schedule.

3. Provision of Corporate Resolution Planning Information

3.1 Paragraphs 3 to 5 shall apply if the Call-Off Contract has been specified as a Critical Service Contract under Paragraph 2.1 or the Supplier is or becomes a Public Sector Dependent Supplier.

3.2 Subject to Paragraphs 3.6, 3.10 and 3.11:

3.2.1 where the Call-Off 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 Start Date; and

3.2.2 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.

3.3 The Supplier shall ensure that the CRP Information provided pursuant to Paragraphs 3.2, 3.8 and 3.9:

3.3.1 is full, comprehensive, accurate and up to date;

3.3.2 is split into three parts:

- (a) Exposure Information (Contracts List);
- (b) Corporate Resolvability Assessment (Structural Review);
- (c) Financial Information and Commentary

and is structured and presented in accordance with the requirements and explanatory notes set out in the latest published version of the Resolution Planning Guidance Note published by the Cabinet Office Government Commercial Function and available at <https://www.gov.uk/government/publications/the-sourcing-and-consultancy-playbooks> and contains the level of detail required (adapted as necessary to the Supplier's circumstances);

3.3.3 incorporates any additional commentary, supporting documents and evidence which would reasonably be required by the Appropriate Authority or Appropriate Authorities to understand and consider the information for approval;

3.3.4 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

3.3.5 complies with the requirements set out at Annex 1 (Exposure Information (Contracts List)), Annex 2 (Corporate Resolvability Assessment (Structural Review)) and Annex 3 (Financial Information and Commentary) respectively.

3.4 Following receipt by the Appropriate Authority or Appropriate Authorities of the CRP Information pursuant to Paragraphs 3.2, 3.8 and 3.9, 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 approve the CRP Information or that the Appropriate Authority or Appropriate Authorities reject the CRP Information.

3.5 If the Appropriate Authority or Appropriate Authorities reject the CRP Information:

3.5.1 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

3.5.2 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 3.3 to 3.5 shall apply again to any resubmitted CRP Information provided that either Party may refer any disputed matters for resolution under clause 32 of the Framework Agreement (Managing disputes).

3.6 Where the Supplier or a member of the Supplier Group has already provided CRP Information to a central government body 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 central government body 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 3.7 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 3.2 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.

3.7 An Assurance shall be deemed Valid for the purposes of Paragraph 3.6 if:

3.7.1 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

3.7.2 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 Call-Off Contract had then been in force) have occurred since the date of issue of the Assurance.

3.8 If the Call-Off Contract is a Critical Service Contract, the Supplier shall provide an updated version of the CRP Information (or, in the case of Paragraph 3.8.3 of its initial CRP Information) to the Appropriate Authority or Appropriate Authorities:

3.8.1 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 3.11) unless the Supplier is relieved of the consequences of the Financial Distress Event as a result of credit ratings being revised upwards;

3.8.2 within 30 days of a Corporate Change Event unless

(a) the Supplier requests and the Appropriate Authority (acting reasonably) agrees to a Corporate Change Event Grace Period, in the event of which the time period for the Supplier to comply with this Paragraph shall be extended as determined by the Appropriate Authority (acting reasonably) but shall in any case be no longer than six months after the Corporate Change Event. During a Corporate Change Event Grace Period the Supplier shall regularly and fully engage with the Appropriate Authority to enable it to understand the nature of the Corporate Change Event and the Appropriate Authority shall reserve the right to terminate a Corporate Change Event Grace Period at any time if the Supplier fails to comply with this Paragraph; or

(b) not required pursuant to Paragraph 3.10;

3.8.3 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 3.10; or

(b) none of the credit rating agencies specified at Paragraph 3.10 hold a public credit rating for the Supplier or any of its Parent Undertakings; and

3.8.4 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 3.8.1 3.8.2 or 3.8.3 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 3.8.4; or

(b) not required pursuant to Paragraph 3.10.

3.9 Where the Supplier is a Public Sector Dependent Supplier and the Call-Off Contract is not a Critical Service Contract, then on the occurrence of any of the events specified in Paragraphs 3.8.1 to 3.8.4, the Supplier shall provide at the request of the Appropriate Authority or Appropriate Authorities and within the applicable timescales for each event as set out in Paragraph 3.8 (or such longer timescales as may be notified to the Supplier by the Buyer), the CRP Information to the Appropriate Authority or Appropriate Authorities.

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

3.10.1 Aa3 or better from Moody's;

3.10.2 AA- or better from Standard and Poors;

3.10.3 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 due to credit ratings being revised upwards) or (ii) the Supplier and its Parent Undertakings cease to fulfil the criteria set out in this Paragraph 3.10, in which cases the Supplier shall provide the updated version of the CRP Information in accordance with paragraph 3.8.

3.11 Subject to Paragraph 5, 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 3.8.

4. Termination Rights

4.1 The Buyer shall be entitled to terminate the Call-Off Contract if the Supplier is required to provide CRP Information under Paragraph 3 and either:

4.1.1 the Supplier fails to provide the CRP Information within 4 months of the Start Date if this is a Critical Service Contract or otherwise within 4 months of the Appropriate Authority's or Appropriate Authorities' request; or

4.1.2 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 Call-Off Contract, which shall be deemed to be an event to which Clause 18.4 applies.

5. Confidentiality and usage of CRP Information

5.1 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.

5.2 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 5.1 and incorporated Framework Agreement clause 34.

5.3 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 3 subject, where necessary, to the Appropriate Authority or Appropriate Authorities entering into an appropriate confidentiality agreement in the form required by the third party.

5.4 Where the Supplier is unable to procure consent pursuant to Paragraph 5.3, 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:

5.4.1 redacting only those parts of the information which are subject to such obligations of confidentiality;

5.4.2 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

5.5 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.

ANNEX 1: EXPOSURE: CRITICAL CONTRACTS LIST

1 The Supplier shall:

1.1 provide details of all agreements held by members of the Supplier Group where those agreements are for goods, services or works provision and:

(a) are with any UK public sector bodies including: central government departments and their arms-length bodies and agencies, non-departmental public bodies, NHS bodies, local buyers, health bodies, police fire and rescue, education bodies and the devolved administrations;

(b) are with any private sector entities where the end recipient of the service, goods or works provision is any of the bodies set out in Paragraph 1.1(a) of this Annex 1 and where the member of the Supplier Group is acting as a key sub-contractor under the contract with the end recipient; or

(c) 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

ANNEX 2: CORPORATE RESOLVABILITY ASSESSMENT (STRUCTURAL REVIEW)

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 agreements listed pursuant to Annex 1 if the Supplier or another member of the Supplier Group is subject to an Insolvency Event;

1.2 ensure that the information is presented so as to provide a simple, effective and easily understood overview of the Supplier Group; and

1.3 provide full details of the importance of each member of the Supplier Group to the Supplier Group's UK Public Sector Business and CNI agreements listed pursuant to Annex 1 and the dependencies between each.

ANNEX 3: Financial information AND COMMENTARY

1 The Supplier shall:

1.1 provide sufficient financial information for the Supplier Group level, contracting operating entities level, and shared services entities' level to allow the Appropriate Authority to understand the current financial interconnectedness of the Supplier Group and the current performance of the Supplier as a standalone entity; and

1.2 ensure that the information is presented in a simple, effective and easily understood manner.

2 For the avoidance of doubt the financial information to be provided pursuant to Paragraph 1 of this Annex 3 should be based on the most recent audited accounts for the relevant entities (or interim accounts where available) updated for any material changes since the Accounting Reference Date provided that such accounts are available in a reasonable timeframe to allow the Supplier to comply with its obligations under this Schedule. If such accounts are not available in that timeframe, to the extent permitted by Law financial information should be based on unpublished unaudited accounts or management accounts (disclosure of which to the Appropriate Authority remains protected by confidentiality).

Schedule 9 - Variation Form

This form is to be used in order to change a Call-Off Contract in accordance with Clause 32 (Variation process)

Contract Details		
This variation is between:	[insert name of Buyer] ("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: Buyer/Supplier]	
Variation number:	[insert variation number]	
Date variation is raised:	[insert date]	
Proposed variation		
Reason for the variation:	[insert reason]	
A Variation 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"> [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 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.

Signed by an authorised signatory for and on behalf of the 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

Schedule 10: Security

See separately appended document.



**UBDS
DIGITAL**
A UBDS GROUP COMPANY

SECURE CONNECTIVITY SERVICE OFFERINGS

For G-CLOUD 14

May 2024

Classification: Public

CONTENTS

1 UBDS DIGITAL OVERVIEW.....3

1.1 WHY CLIENTS CHOOSE UBDS DIGITAL.....3

1.2 SERVICES THAT DRIVE INNOVATION3

2 CISCO SOFTWARE DEFINED WAN (SD-WAN) DESIGN, BUILD AND MANAGED SERVICE.4

3 MERAKI SOFTWARE DEFINED WAN (SD-WAN) DESIGN, BUILD AND MANAGED SERVICES.5

4 SILVERPEAK SOFTWARE DEFINED WAN (SD-WAN) DESIGN, BUILD AND MANAGED SERVICE. 6

5 VMWARE VELOCLOUD SOFTWARE DEFINED WAN (SD-WAN) DESIGN, BUILD AND MANAGED SERVICE.....7

6 SOFTWARE DEFINED WAN (SD-WAN) DESIGN, BUILD AND MANAGED SERVICE. 8

7 HOSTED SOFTWARE DEFINED (SD-WAN) – CISCO VIPTELA. 9

8 HOSTED SOFTWARE DEFINED (SD-WAN) – VMWARE VELOCLOUD.10

9 SOFTWARE DEFINED WAN (SD-WAN) AND CLOUD NETWORKING READINESS ASSESSMENT.11

10 SOFTWARE DEFINED WAN (SD-WAN) FOR CLOUD ADOPTION..... 12

11 SOFTWARE DEFINED WAN (SD-WAN) PROOF OF CONCEPT DEPLOYMENT AND BUSINESS CASE..... 13

12 HYBRID, ZERO TRUST AND CLOUD NETWORKING DESIGN, IMPLEMENTATION AND MANAGED SERVICES..... 14

13 NETWORK TRANSFORMATION FOR CLOUD ADOPTION..... 15

14 CLOUD AND ZERO TRUST SECURITY SERVICES. 16

15 CLOUD HYBRID NETWORKING. 17

16 MODERNISE ENDPOINTS. 18

17 MICROSOFT TEAMS PHONE SYSTEM. 19

18 ANYWHERE 365 – CONTACT CENTRE. 20

1 UBDS DIGITAL OVERVIEW.

At UBDS Digital, we recognise that technology must not only be cutting-edge but also practical and quick to implement. We specialise in transforming your complex challenges into opportunities, delivering solutions that are not just acceptable but truly exceptional. Our approach ensures that with us, you navigate the intricacies of digital transformation with unwavering confidence and achieve outcomes that surpass expectations. You will never have to compromise on quality, security, and reliability. That is our promise to you.






1.1 Why clients choose UBDS Digital.

At UBDS Digital, we are on a mission. To deliver unparalleled client value, unmatched employee experience and to make a meaningful difference in society.



1.2 Services that drive innovation

We are smarter in our solutions, more imaginative in our use of technology, more agile in our processes, more rigorous in our security. Below covers our key service offerings across UBDS Digital.

 Digital Consulting <ul style="list-style-type: none"> ▪ Digital Transformation Strategy ▪ User Experience Design ▪ Business Change 	 Cloud <ul style="list-style-type: none"> ▪ Cloud Adoption ▪ Migration and Modernisation ▪ App Development and Innovation 	 Data and AI <ul style="list-style-type: none"> ▪ Data Transformation Strategy ▪ Data Platform Migration and Modernisation ▪ AI Services ▪ Advanced Analytics
 Cybersecurity <ul style="list-style-type: none"> ▪ Risk Assessment and Management ▪ Compliance and Governance 	 Managed Services <ul style="list-style-type: none"> ▪ Secure Connectivity ▪ Cloud Hosting ▪ Modern Workplace and Productivity ▪ Service Management and Transition ▪ FinOps ▪ Security Operations Centre 	 Portfolio, Programme, and Project Management <ul style="list-style-type: none"> ▪ Technology Delivery ▪ PMO Set Up and Management

2 CISCO SOFTWARE DEFINED WAN (SD-WAN) DESIGN, BUILD AND MANAGED SERVICE.

UBDS Digital's Cisco Software Defined WAN (SD-WAN) Service is built on our expertise and success. We have a proven track record of designing, building, transitioning, and managing next-generation Public and Private large enterprise networks using Cisco SD-WAN technologies. Our expertise lies in supporting our clients on their journey to transition rapidly to a Cloud-ready hybrid network. Our ultimate goal is to put them on a path to a 'zero-trust' network, which is highly secure and reliable.

Our service includes the delivery of transition to enterprise-class Cisco SD-WAN directly to your cloud. Our services will complement any existing networking solution you might have in place, and we offer both Cloud and On-Premise Hosting options, depending on your business needs and preferences. We also provide vCPE (Virtual Customer Premise Equipment) support, ensuring that your network is always up and running.

We offer SD-WAN in the cloud, including AWS, Azure and On-Premise. This service delivers hybrid networking and enables zero trust networking, providing you with a secure and reliable network. Our rapid deployment ensures that your sites are online in under five days. We use broadband, fibre and/or mobile to ensure the best possible connection. Our service is fully managed - we take care of everything from order, design, build, transition, operation, and decommissioning.

Our service has many benefits. You will experience improved network reliability and performance, reduced latency impact, and reduced networking costs. You will see improved performance for cloud-based applications, and our service simplifies network integration and secures network transport. We offer Cloud, SaaS, and WAN optimisation, and we are network provider agnostic. Our agile delivery ensures that we are always ready to configure new features and capabilities on your network. With UBDS Digital, you can rest assured that your network is in safe hands.

3 MERAKI SOFTWARE DEFINED WAN (SD-WAN) DESIGN, BUILD AND MANAGED SERVICES.

UBDS Digital's Meraki Software Defined WAN (SD-WAN) Service is built on our expertise and success. We have a proven track record of designing, building, transitioning, and managing next-generation Public and Private large enterprise networks using Cisco Meraki SD-WAN technologies. Our expertise lies in supporting our clients on their journey to transition rapidly to a Cloud-ready hybrid network. Our ultimate goal is to put them on a path to a 'zero-trust' network, which is highly secure and reliable.

Our service includes the delivery of transition to enterprise-class Meraki SD-WAN directly to your cloud. Our services will complement any existing networking solution you might have in place, and we offer both Cloud and On-Premise Hosting options, depending on your business needs and preferences. We also provide vCPE (Virtual Customer Premise Equipment) support, ensuring that your network is always up and running.

We offer SD-WAN in the cloud, including AWS, Azure and On-Premise. This service delivers hybrid networking and enables zero trust networking, providing you with a secure and reliable network. Our rapid deployment ensures that your sites are online in under five days. We use broadband, fibre and/or mobile to ensure the best possible connection. Our service is fully managed - we take care of everything from order, design, build, transition, operation, and decommissioning.

Our service has many benefits. You will experience improved network reliability and performance, reduced latency impact, and reduced networking costs. You will see improved performance for cloud-based applications, and our service simplifies network integration and secures network transport. We offer Cloud, SaaS, and WAN optimisation, and we are network provider agnostic. Our agile delivery ensures that we are always ready to configure new features and capabilities on your network. With UBDS Digital, you can rest assured that your network is in safe hands.

4 SILVERPEAK SOFTWARE DEFINED WAN (SD-WAN) DESIGN, BUILD AND MANAGED SERVICE.

UBDS Digital's Silverpeak Software Defined WAN (SD-WAN) Service is built on our expertise and success. We have a proven track record of designing, building, transitioning, and managing next-generation Public and Private large enterprise networks using Silverpeak SD-WAN technologies. Our expertise lies in supporting our clients on their journey to transition rapidly to a Cloud-ready hybrid network. Our ultimate goal is to put them on a path to a 'zero-trust' network, which is highly secure and reliable.

Our service includes the delivery of transition to enterprise-class Silverpeak SD-WAN directly to your cloud. Our services will complement any existing networking solution you might have in place. and we offer both Cloud and On-Premise Hosting options, depending on your business needs and preferences. We also provide vCPE (Virtual Customer Premise Equipment) support, ensuring that your network is always up and running.

We offer SD-WAN in the cloud, including AWS, Azure and On-Premise. This service delivers hybrid networking and enables zero trust networking, providing you with a secure and reliable network. Our rapid deployment ensures that your sites are online in under five days. We use broadband, fibre and/or mobile to ensure the best possible connection. Our service is fully managed - we take care of everything from order, design, build, transition, operation, and decommissioning.

Our service has many benefits. You will experience improved network reliability and performance, reduced latency impact, and reduced networking costs. You will see improved performance for cloud-based applications, and our service simplifies network integration and secures network transport. We offer Cloud, SaaS, and WAN optimisation, and we are network provider agnostic. Our agile delivery ensures that we are always ready to configure new features and capabilities on your network. With UBDS Digital, you can rest assured that your network is in good hands.

5 VMWARE VELOCLOUD SOFTWARE DEFINED WAN (SD-WAN) DESIGN, BUILD AND MANAGED SERVICE.

UBDS Digital's VMware Velocloud Software Defined WAN (SD-WAN) Service is built on our expertise and success. We have a proven track record of designing, building, transitioning, and managing next-generation Public and Private large enterprise networks using VMware Velocloud SD-WAN technologies. Our expertise lies in supporting our clients on their journey to transition rapidly to a Cloud-ready hybrid network. Our ultimate goal is to put them on a path to a 'zero-trust' network, which is highly secure and reliable.

Our service includes the delivery of transition to enterprise-class VMware Velocloud SD-WAN directly to your cloud. Our services will complement any existing networking solution you might have in place. and we offer both Cloud and On-Premise Hosting options, depending on your business needs and preferences. We also provide vCPE (Virtual Customer Premise Equipment) support, ensuring that your network is always up and running.

We offer SD-WAN in the cloud, including AWS, Azure and On-Premise. This service delivers hybrid networking and enables zero trust networking, providing you with a secure and reliable network. Our rapid deployment ensures that your sites are online in under five days. We use broadband, fibre and/or mobile to ensure the best possible connection. Our service is fully managed - we take care of everything from order, design, build, transition, operation, and decommissioning.

Our service has many benefits. You will experience improved network reliability and performance, reduced latency impact, and reduced networking costs. You will see improved performance for cloud-based applications, and our service simplifies network integration and secures network transport. We offer Cloud, SaaS, and WAN optimisation, and we are network provider agnostic. Our agile delivery ensures that we are always ready to configure new features and capabilities on your network. With UBDS Digital, you can rest assured that your network is in good hands.

6 SOFTWARE DEFINED WAN (SD-WAN) DESIGN, BUILD AND MANAGED SERVICE.

UBDS Digital's Software Defined WAN (SD-WAN) Service is built on our expertise and success. We have a proven track record of designing, building, transitioning, and managing next-generation Public and Private large enterprise networks using SD-WAN technologies. Our expertise lies in supporting our clients on their journey to transition rapidly to a Cloud-ready hybrid network. Our ultimate goal is to put them on a path to a 'zero-trust' network, which is highly secure and reliable.

Our service includes the delivery of transition to enterprise-class SD-WAN directly to your cloud. Our services will complement any existing networking solution you might have in place. and we offer both Cloud and On-Premise Hosting options, depending on your business needs and preferences. We also provide vCPE (Virtual Customer Premise Equipment) support, ensuring that your network is always up and running.

We offer SD-WAN in the cloud, including AWS, Azure and On-Premise. This service delivers hybrid networking and enables zero trust networking, providing you with a secure and reliable network. Our rapid deployment ensures that your sites are online in under five days. We use broadband, fibre and/or mobile to ensure the best possible connection. Our service is fully managed - we take care of everything from order, design, build, transition, operation, and decommissioning.

Our service has many benefits. You will experience improved network reliability and performance, reduced latency impact, and reduced networking costs. You will see improved performance for cloud-based applications, and our service simplifies network integration and secures network transport. We offer Cloud, SaaS, and WAN optimisation, and we are network provider agnostic. Our agile delivery ensures that we are always ready to configure new features and capabilities on your network. With UBDS Digital, you can rest assured that your network is in good hands.

7 HOSTED SOFTWARE DEFINED (SD-WAN) – CISCO VIPTELA.

UBDS Digital has a proven track record in the design, construction, transition, and management of next-generation public and private large enterprise networks. We have achieved this by leveraging the power and capabilities of Cisco Viptela SD-WAN technologies. Our primary goal is to support our clients on their journey to rapidly transition to a Cloud-ready hybrid network. This transition is not just about technology, but it also puts them on a path to a zero-trust network that is highly secure and reliable.

One of the key features of our service is the delivery of transition to enterprise class Software-Defined Networking (SD-WAN). This allows us to bring SD-WAN directly to your cloud, complementing any existing networking solution you may have. We also offer Cloud or On-Premise Orchestrator/Controller Hosting, providing you with the flexibility to choose the hosting solution that best suits your needs.

UBDS Digital provides you with vCPE (Virtual Customer Premise Equipment) support, which is essential for the smooth operation of your network. We offer SD-WAN in the cloud, including AWS, Azure and On-Premise. This delivers hybrid networking and enables zero trust networking. We enable rapid deployment, with pop up sites going online in just a few days. Our service uses broadband, fibre and/or mobile and is a fully managed service. We take care of everything from order to design, build, transition, operate, and decommissioning.

Our service offers many benefits. You will experience improved network reliability and performance, reduced latency impact, and lower networking costs. Your application performance will improve, especially for cloud-based applications. Network integration will be simplified, and network transport will be secured, and you will also benefit from Cloud, SaaS, and WAN optimisation. We are Network Provider agnostic, working with any provider. Finally, our service is agile, allowing us to configure new features capabilities on your network.

8 HOSTED SOFTWARE DEFINED (SD-WAN) – VMWARE VELOCLOUD.

UBDS Digital has a proven track record in the design, construction, transition, and management of next-generation public and private large enterprise networks. We have achieved this by leveraging the power and capabilities of VMware Velocloud technologies. Our primary goal is to support our clients on their journey to rapidly transition to a Cloud-ready hybrid network. This transition is not just about technology, but it also puts them on a path to a zero-trust network that is highly secure and reliable.

One of the key features of our service is the delivery of transition to enterprise class Software-Defined Networking (SD-WAN). This allows us to bring SD-WAN directly to your cloud, complementing any existing networking solution you may have. We also offer Cloud or On-Premise Orchestrator/Controller Hosting, providing you with the flexibility to choose the hosting solution that best suits your needs.

UBDS Digital provides you with vCPE (Virtual Customer Premise Equipment) support, which is essential for the smooth operation of your network. We offer SD-WAN in the cloud, including AWS, Azure and On-Premise. This delivers hybrid networking and enables zero trust networking. We enable rapid deployment, with pop up sites going online in just a few days. Our service uses broadband, fibre and/or mobile and is a fully managed service. We take care of everything from order to design, build, transition, operate, and decommissioning.

Our service offers many benefits. You will experience improved network reliability and performance, reduced latency impact, and lower networking costs. Your application performance will improve, especially for cloud-based applications. Network integration will be simplified, and network transport will be secured, and you will also benefit from Cloud, SaaS, and WAN optimisation. We are Network Provider agnostic, working with any provider. Finally, our service is agile, allowing us to configure new features capabilities on your network.

9 SOFTWARE DEFINED WAN (SD-WAN) AND CLOUD NETWORKING READINESS ASSESSMENT.

UBDS Digital's Software Defined WAN (SD-WAN) and Cloud Networking Readiness Assessment is a comprehensive service that enables organisations to fully understand the case, opportunities, and investments required to transform their network to support cloud-based networking and/or SD-WAN. This service is designed to help customers navigate the complexities of network transformation, providing them with the necessary knowledge and tools to make informed decisions.

Our team of experts will help you to develop a strategy and business case, working through the technology, service experience, economic, financial and management cases. Our business cases comply with the Treasury Green Book Five-Case Model, ensuring that they meet the highest standards of financial and economic analysis. Our work involves a thorough analysis of the current network infrastructure, identifying areas for improvement and potential challenges, and providing recommendations for the best path forward.

The assessment will define the Cloud networking requirements needed to meet Cloud services. This is a critical step in ensuring that the network is capable of supporting the demands of Cloud-based services. The assessment is also aligned to security best practice and guidance, ensuring that the network transformation does not compromise the security of the organisation's data and systems.

We will create a technology blueprint and roadmap, which outlines the steps necessary to achieve the desired network transformation. We also define the transition approach and plan, and the benefits case, providing a clear picture of the potential benefits and returns on investment.

In addition, we will assess capability readiness, in terms of people and process, and the optimal financial approach, including funding and expected total cost. We identify the most suitable commercial routes for procurement, ensuring that the network transformation is cost-effective and delivers value for money.

The benefits of our assessment service include access to some of the UK's leading Cloud Network architects and engineers, and hundreds of years of combined cloud experience working with leading vendors. We provide a tailored approach to reach your business-outcome, ensuring that the solution is right for your organisation. Our rapid, holistic approach allows us to develop outline cases within extremely short timescales by leveraging our proven experience, enabling you to prepare to mobilise and commence execution immediately.

10 SOFTWARE DEFINED WAN (SD-WAN) FOR CLOUD ADOPTION.

UBDS Digital has a proven track record in expertly designing, building, transitioning, and managing large enterprise networks using advanced SD-WAN technologies. We are committed to supporting our clients on their journey to transition rapidly to a Cloud-ready hybrid network. We provide the expertise and experience to put organisations on a path towards a zero-trust network.

Our service includes the transition to enterprise class Software-Defined Networking (SD-WAN). We can bring SD-WAN directly to your cloud, making it a seamless integration. Our service is complementary to any existing networking solution you may already have in place, ensuring a smooth transition with no disruption to your operations.

We offer Cloud and On-Premise Hosting, giving you the flexibility to choose the option that best suits your business needs. We also provide support for vCPE (Virtual Customer Premise Equipment) and NSX.

Our SD-WAN solutions can be deployed in the cloud, including platforms such as AWS, Azure, and On-Premise. This allows us to deliver hybrid networking and enable zero trust networking, providing you with a secure and reliable network infrastructure.

We pride ourselves on our rapid deployment capabilities, with sites being online in under five days. Our SD-WAN solutions can utilise broadband, fibre, and/or mobile connections, providing you with a range of options to suit your specific needs.

We offer a fully managed service that covers everything from order through to design, build, transition, operate, and decommissioning. This ensures that you can focus on your core business while we take care of your networking needs.

There are many benefits of our SD-WAN services. They can significantly improve network reliability and performance, reduce latency impact, and cut networking costs. They can also enhance application performance, particularly for cloud-based applications, simplify network integration, secure network transport, and optimise Cloud, SaaS, and WAN. Our solutions are network provider agnostic and offer agile delivery, allowing us to configure new features and capabilities on your network.

11 SOFTWARE DEFINED WAN (SD-WAN) PROOF OF CONCEPT DEPLOYMENT AND BUSINESS CASE.

Our service provides organisations who are considering the implementation of Software Defined WAN (SD-WAN), with the opportunity to leverage the expertise of UBDS to build a Proof of Concept (PoC). This PoC can typically be implemented across various sites within a span of 2-4 weeks and can be overlaid on your existing network. The PoC provides you with a unique opportunity to thoroughly test SD-WAN and establish the tangible benefits it will deliver to your business operations.

The features of our SD-WAN PoC are numerous. We offer rapid deployment, with sites online in under five days, ensuring minimal disruption to your business operations. We also provide a managed transition to enterprise-class Software-Defined Networking (SD-WAN). Our SD-WAN solution can be directly linked to your cloud and is complementary to any existing networking solution you may have.

We offer cloud and on-premise hosting options, providing flexibility based on your business needs. Our solution supports vCPE and NSX, and can be extended to platforms such as AWS, VMware, Hyper-V, and more. Our SD-WAN solution delivers hybrid networking, utilising your existing broadband, fibre, and/or mobile connectivity. We offer a fully managed service from the point of order to decommissioning, ensuring a hassle-free experience for you.

There are many benefits of our SD-WAN PoC. It allows you to test drive the solution before making a substantial investment. It improves network reliability and performance, reducing latency impact and network costs. It enhances application performance, particularly for cloud-based applications. It simplifies network integration, making it easier for your IT team to manage. Our solution also optimises cloud, SAS, and WAN, and ensures secure network transport. Finally, our solution is network provider agnostic, meaning it can work with any provider you currently use or use in the future.

12 HYBRID, ZERO TRUST AND CLOUD NETWORKING DESIGN, IMPLEMENTATION AND MANAGED SERVICES.

UBDS Digital is a leading provider of hybrid, zero trust, and cloud networking design, implementation, and managed services. We specialise in designing, building, transitioning to, and managing next-generation cloud networking technologies, supporting our clients on their journey to transition rapidly to a cloud-ready hybrid network. Ultimately, we guide organisations on a path to a zero-trust network. We offer a wide range of solutions from LAN to SD-WAN to CASB, working with vendors like Cisco, HPE, VMware, and ZScaler.

Our service includes assessing applications and infrastructure to support hybrid and zero-trust networks, along with strategy, design, and execution. We conduct a cloud and zero trust readiness assessment of applications and servers. We define security plans and controls, conduct risk assessments, and implement them. We provide cloud, SD WAN, and zero trust high-level/detailed network designs and take end-to-end responsibility across LAN, Wi-Fi, SDWAN, and CASB. UBDS also offers design, implementation, and managed service support for LAN and Wi-Fi. We are vendor agnostic, working with Cisco Meraki, HP Aruba, Ubiquiti, Dell, ZScaler, and VMware. Throughout all our services we provide knowledge transfer and training to your staff.

The benefits of working with us are numerous. We are home to the UK's leading cloud network architects and engineers with hundreds of years of combined cloud experience working with leading vendors. Our architects and engineers are leading subject matter network experts. We take a rapid and holistic approach, developing outline cases within short timescales and leverage our proven experience in building business cases and technology roadmaps. We enable you to prepare for mobilisation and commence execution immediately. In short, organisations can be safe in the knowledge that they can trust UBDS Digital for all their hybrid, zero trust, and cloud networking design, implementation, and managed service needs.

13 NETWORK TRANSFORMATION FOR CLOUD ADOPTION.

UBDS Digital is a leading provider of network transformation services for cloud adoption. We assist organisations in planning, designing, and implementing highly resilient and secure cloud-based services. Our managed architecture services are designed to support organisations in transforming their IT operating model, developing their IT roadmap, establishing integration capabilities, and creating implementation and transition plans to migrate from existing architecture to the cloud. We take a technology-agnostic approach and align our services with industry frameworks and methodologies.

Our services include strategy, architecture, and ROI support for transition to the cloud. We provide technical solution design and validation to support the transition process. We conduct architecture capability assessment and improvement planning to ensure that your organisation is ready for the cloud transition. We also offer programme management and transformation planning with knowledge transfer to ensure that your team is equipped with the necessary skills and knowledge for the transition.

We support you throughout adoption from the start, providing evaluation and advice on Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) adoption. We then create architectural blueprints, roadmaps, governance, transition planning, high/low level designs to guide your organisation through the cloud transition process. We will enable you to create an architectural vision that includes cloud and digital service strategies and a readiness assessment.

We assist in the transition from heritage legacy infrastructure including network, remote access, and datacentre and we design and implement new network topologies such as Software-Defined Wide Area Network (SD-WAN) and Cloud Access Security Broker (CASB). We also support the incubation and adoption of Site Reliability Engineering.

The benefits of our services include a flexible, scalable, independent, technology-agnostic approach. We have multi-disciplinary expertise with extensive supply/client-side experience in complex environments. We offer multiple delivery options providing flexible and bespoke architecture solutions. We have extensive experience in Public, Private, Hybrid Cloud and digital services.

Our service will help in reducing the cost of migration to the cloud and legacy rationalisation (networks). Our cloud solutions are aligned to business drivers, maximising efficiency, and ROI. Our expertise is aligned with best practice architecture standards/frameworks such as The Open Group Architecture Framework (TOGAF) and Zachman Framework and we assist you in moving to an Agile delivery model from IT Service Management (ITSM). We have a proven track record of success in operating a Cloud Centre of Excellence and the expertise to transition your organisation to the cloud.

14 CLOUD AND ZERO TRUST SECURITY SERVICES.

UBDS Digital has a proven track record of designing, building, transitioning to, and managing next-generation large enterprise networks using SD-WAN technologies. We are known for our expertise in supporting organisations on their journey to transition rapidly to a Cloud-ready hybrid network and ultimately to put them on a path to a zero-trust network. Zero trust is a network model that requires all users, even those inside the organisation's enterprise network, to be authenticated, authorised, and continuously validating security configuration and posture, before being granted or keeping access to applications and data.

Our services feature the design and integration of active and passive preventative security products and controls. We assess, architect, and deploy business policies, solutions, privacy, and data. We ensure provable compliance using a real-time, zero trust based model. We also offer application and server micro-segmentation, a method of creating zones in data centres and cloud environments that isolate workloads from one another and secure them individually.

Our services also include simple and powerful off-server forensic evidence toolsets, third-party supplier assurance, and adherence to international compliance standards and GDPR practitioners. We follow National Standards NCSC Cloud security principles, CAST, PSN, LI, and HSCN. We also help identify the best mix of security products to deploy, based on the unique needs of each client.

There are multiple benefits of using our services. We provide an independent, unbiased technology agnostic assessment and offer a relevant security design approach that supports cloud and zero trust networking. We help reduce risk by applying real-world experience and increasing confidence in the security measures implemented. Our services provide on-demand evidence, removing the necessity for expensive, single-use audits. We also offer preventative automated enforcement, controlling application usage and network attacks.

We can reduce RCA to hours, not weeks, gaining control and confidence. We have a deep understanding of unique UK policies, which helps expedite service approvals. Our services are human-managed and machine-driven, providing more visibility with fewer overheads. Finally, we offer shorter design and delivery phases by leveraging templated baselines.

15 CLOUD HYBRID NETWORKING.

At UBDS Digital, we understand that Cloud native services, while highly beneficial, may not always be feature-rich enough to meet all your needs. This is why we sometimes find it necessary to build systems based on Commercial Off-The-Shelf (COTS) products. One example of this is the implementation of Next Generation Firewalls in the Cloud. These are designed to ensure that services like third-party VPNs, BGP routing, and SD-WAN integration can be adequately supported, providing a robust and secure network infrastructure.

UBDS Digital's Cloud Hybrid Networking service features a private high-speed connection from your on-premises data centre to the Cloud. This ensures a seamless and efficient data transfer, reducing latency and improving overall system performance. We offer AWS Direct Connect and Azure Express Route integration services. AWS Direct Connect provides a dedicated network connection from your premises to AWS, helping to reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections.

Azure Express Route enables you to extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. This can offer lower latencies and higher security than typical connections over the internet.

We also offer SD-WAN integration services. This allows for the integration of your SD-WAN directly to the Cloud, providing a secure, high-performance connection. Additionally, our Zscaler private access integration services provide secure access to internally managed applications without exposing your network to the internet.

One of the significant benefits of our services is the high-speed secure connectivity from your data centre to the Cloud. This ensures that your data is transferred quickly and securely, reducing the risk of data breaches. Our direct connections to AWS Transit Hub and VPC infrastructure, and Azure Hub and VNET infrastructure, ensure seamless integration with these platforms.

UBDS Digital understands the importance of providing the best user experience for remote workers accessing Cloud-hosted applications. Our tailored Cloud solutions are designed to meet your business demands, ensuring that your remote workers can access the applications they need quickly and efficiently. We also provide separation and Firewall control for third-party connectivity, ensuring that your network remains secure even when integrating with third-party services. Finally, our design and provision of Hub and Spoke design ensure a robust and efficient network infrastructure.

16 MODERNISE ENDPOINTS.

In the face of the continuous transformation of today's business scenarios, a fresh and innovative approach is required to cater to the needs of hybrid work environments, frontline workers, and the implementation of a Zero Trust security model. UBDS Digital has the expertise and experience to assess, deploy, and provide support for your Microsoft 365 Endpoint modernisation journey. This could involve physical computing or virtual cloud desktops, depending on your specific needs and requirements.

Our modernisation process includes many beneficial features. The endpoints are cloud-connected and built on the robust foundation of M365, coupled with an intelligent security cloud. This ensures a high level of security and efficiency. With Endpoint Manager, you can plan, deploy, and configure applications with ease and precision. The deployment process is streamlined with zero touch provisioning, making it hassle-free and efficient.

Our service also covers transforming remote computing with the help of Windows 365 and Azure Virtual Desktop. This transformation enhances the efficiency and effectiveness of remote work. We include a thorough review of company policies and device scenarios to ensure optimal performance. Licensing is also reviewed to ensure compliance and cost-effectiveness. The architecture design is another crucial aspect of our service, ensuring a robust and efficient system.

There are many benefits of our Endpoint modernisation service. It results in significant IT administration and deployment savings, reducing costs and increasing efficiency. Vendor license and cost consolidation is another major benefit, leading to further cost reductions. The service leads to automation and process improvement, enhancing efficiency and productivity. The total cost of risk is also reduced, providing financial benefits. The modernisation process also results in a flexible workspace with secure access to data, enhancing productivity and security, with device management, automation, consolidation, and cost reduction are other major benefits.

17 MICROSOFT TEAMS PHONE SYSTEM.

The Microsoft Teams Phone System is a comprehensive solution that provides full PBX capabilities in a single, all-inclusive package. This enterprise-grade phone system comes equipped with many standard features that you would expect from a traditional phone system, including voice mail, caller ID, shared phone lines, and emergency calling.

In addition to these standard features, the Microsoft Teams Phone System also supports advanced call handling. This is made possible through the use of AutoAttendants, also known as Interactive Voice Response (IVR) systems, and Call Queues. These features allow for efficient call routing and handling, ensuring that calls are directed to the appropriate person or department.

The Microsoft Teams Phone System is a cloud-based PBX service. This means that it can be accessed from any device that is Teams enabled or capable. It supports PSTN Dialling via direct routing, calling plans or operator connect. It also features a cloud voicemail system, calling line identification, pickup groups (call groups), and hunt groups (call queues).

The IVR (Auto Attendants) feature allows for automated call handling, while blind and consultative transfers enable seamless call transfers. The system can also be enhanced by third-party switchboard and contact centre applications.

One of the main benefits of the Microsoft Teams Phone System is that it is an all-in-one solution. This means that there is no need for additional infrastructure investment. Users can have a single phone number across their computer, mobile and desk phone.

The system also offers a range of devices built specifically for Teams, simplifying management through existing Teams interfaces. Reporting features are included, and the system integrates with Microsoft Teams Rooms (MTR).

The Microsoft Teams Phone System is delivered as a full end-to-end service, operating on an Opex operating model. It offers improved resilience and uptime with built-in redundancy and load balancing. This ensures that the system remains operational and efficient, even during periods of high demand or unexpected disruptions.

18 ANYWHERE 365 – CONTACT CENTRE.

UBDS Digital's Anywhere 365 service enables digital transformation of your contact centre. We will deliver a Microsoft Teams-enabled omni-channel contact centre solution based on the Anywhere 365 Dialogue Cloud range of services. Our comprehensive offering provides an end-to-end service from the initial discovery phase, through to the design, implementation, training, and, finally, handover to service.

Our service is a Microsoft Teams-enabled omnichannel contact centre that is cloud-based and fully integrated with the Teams Phone System Direct Routing. The omni-channel routing feature allows for routing based on skills, as well as Interactive Voice Response (IVR) prompts. Real-time metrics and reporting are available via Power BI, providing valuable insights and data for your business. For compliance and training purposes, call recording is also included. Our service can support Customer Relationship Management (CRM) integration, further enhancing its functionality.

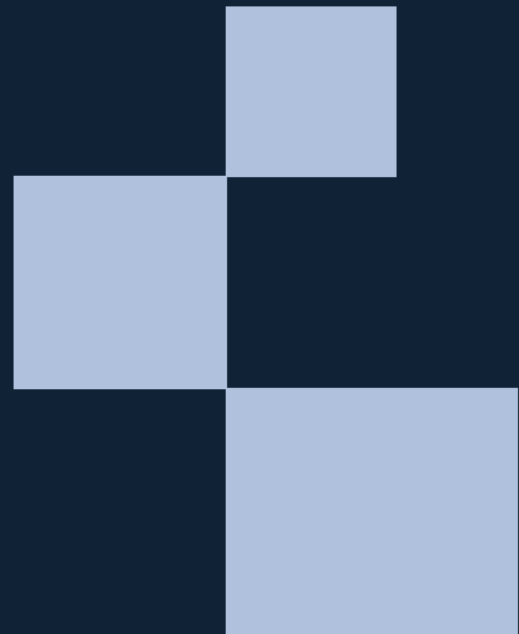
Our team provides a full end-to-end design and delivery service, ensuring a seamless transition and implementation. A fully managed service is also available, taking the burden off your team. The range of licensing levels supports all sizes of contact centres, making it a versatile solution for businesses of all scales. The service is easy to scale and to develop additional capability for via Power Automate, providing flexibility and adaptability.

There are multiple benefits of moving to Anywhere 365. It enhances your Microsoft 365 investment by building on a single platform, reducing operating and management costs. It improves agent performance with a single Teams-based application and moves to a truly location-independent model. Real-time metrics allow for enhanced customer service and a flexible OPEX pricing model. It also improves business decision-making with in-depth data analysis, and it integrates seamlessly into other 3rd Party solutions. Finally, it provides a single platform for all customer contact channels and is easy to scale up and down as needed.



UBDS
DIGITAL
A UBDS GROUP COMPANY

**EXCEPTIONAL OUTCOMES.
NEVER COMPROMISE.**





Crown
Commercial
Service

Statement of Requirements

Contract Reference: P3389 UKSV Network Infrastructure Review

CONTENTS

1. PURPOSE	3
2. BACKGROUND TO THE BUYER	3
3. BACKGROUND/OVERVIEW OF THE REQUIREMENT	3
4. DEFINITIONS	4
5. SCOPE OF REQUIREMENT	4
6. THE REQUIREMENT	4
7. KEY MILESTONES AND DELIVERABLES	4
8. MANAGEMENT INFORMATION/REPORTING	5
9. VOLUMES	5
10. CONTINUOUS IMPROVEMENT	5
11. SUSTAINABILITY/ SOCIAL VALUE	6
12. QUALITY	6
13. PRICE	6
14. STAFF AND CUSTOMER SERVICE	6
15. SERVICE LEVELS AND PERFORMANCE	7
16. SECURITY AND CONFIDENTIALITY REQUIREMENTS	7
17. PAYMENT AND INVOICING	7
18. CONTRACT MANAGEMENT	7
19. INTELLECTUAL PROPERTY RIGHTS	8
20. LOCATION	8

OFFICIAL

1. PURPOSE

- 1.1 UKSV (part of the Cabinet office) are seeking an organisation who specialise in Infrastructure/network reviews. This supplier will provide specialist in-depth understanding of the services that UKSV use and the existing connectivity from UKSV [REDACTED]

2. BACKGROUND TO THE BUYER

- 2.1 [REDACTED]
- 2.2 BACKGROUND/OVERVIEW OF THE REQUIREMENT
- 2.3 UKSV are seeking an organisation who specialise in Infrastructure/network reviews.
- 2.4 The supplier will provide initial engagement with both key internal and external stakeholders. The supplier will be expected to carry out the services in 2 phases and will include reporting outcomes.
- 2.5 Phase 1 - Discovery sessions, and phase 2 reporting outputs.
- 2.6 [REDACTED]

3. DEFINITIONS

Expression or Acronym	Definition
UKSV	means UK Security Vetting
[REDACTED]	[REDACTED]

4. SCOPE OF REQUIREMENT

- 4.1 UKSV are seeking a supplier that can deliver the requirements set out in section 6 below.

5. THE REQUIREMENT

- 5.1 We are looking for a supplier that can deliver the following requirements:
- 5.2 Phase 1 UKVS Initial Engagement SoR
- 5.3 Discovery – Engagement sessions to be held with key stakeholders at MoD, BT and CGI to gain an in depth understanding of the services that UKSV use

OFFICIAL

and the existing connectivity from UKSV to these services covering the following amongst others:

- Gateways/Proxies - including Hanslope Park PNC Terminal
- Network Connectivity to Third Party services
- Security Policies
- Access Controls/Authentication
- DNS
- FQDN's
- IP Addressing
- Resilience
- Bandwidth/utilization/throughput

5.4 Phase 2 Reporting Outputs

5.5 From the information gathered through the Discovery phase a report/roadmap will be produced that will cover the following amongst others:

- End-to-End network diagram(s) for all services
- Details of Gateways/Proxies configuration
- Details of the end-to-end Network Connectivity to Third Party services
- Definition of the Security Policies applied across the end-to-end services
- Details of any Access Controls/Authentication applied to user access of services
- Details of DNS services used
- Details of the FQDN's used for access to all services
- Details of the IP Addressing used for access to all services
- Detail path resilience end to end
- Detail the current Bandwidth/utilization/throughput for paths for each service

5.6 The supplier will ensure they are accredited with the following:

- Cyber Essentials plus
- Security certification ISO27001

5.7 Please note any future design options are out of scope for this Statement of requirements.

OFFICIAL

6. KEY MILESTONES AND DELIVERABLES

The successful supplier will be expected to work with UKSV on an innovative approach to assist us in strategic design and asset work to achieve the below deliverables.

6.1 The key deliverables will be:

6.1.1 Discovery and engagement with MOD, BT, CGI and relevant internal UKSV key stakeholders.

6.1.2 From the information gathered through the Discovery phase a report/roadmap will be produced that will cover the requirements as at section 6.5 above.

6.1.3 The following Contract milestones/deliverables shall apply:

Milestone/ Deliverable	Description	Timeframe or Delivery Date
Phase 1 (Initial Engagement)	Discovery engagement (external and internal stakeholders)	Within three months of contract award
Phase 2 (Reporting outputs)	Reporting outputs including roadmap	Within six months of Contract Award

7. MANAGEMENT INFORMATION/REPORTING

7.1 N/A

8. VOLUMES

8.1 The volumes of work required are as at section 7 'key milestones and deliverables'.

9. CONTINUOUS IMPROVEMENT

9.1 The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

9.2 The Supplier should present new ways of working to the Buyer during Contract review meetings.

OFFICIAL

- 9.3 Changes to the way in which the Services are to be delivered must be brought to the Buyer's attention and agreed prior to any changes being implemented.

10. SUSTAINABILITY/ SOCIAL VALUE

- 10.1 Details of sustainability under this contract should include as an example, consideration on whether or not travelling to a site to deliver the objectives are wholly necessary or whether deliverables can be achieved virtually. In addition the supplier should work with the Buyer throughout the contract to highlight any other sustainability considerations Potential Suppliers can achieve as part of their service offering.
- 11.2 Suppliers delivering this contract should be familiar with Procurement Policy Note (PPN) 6/20 – Taking Account of Social Value in the Award of Central Government Contracts and where appropriate consider additional benefits that can delivered
- 11.3 PPN 06/20 guidance documents can be found at: <https://www.gov.uk/government/publications/procurement-policy-note-0620-taking-account-of-social-value-in-the-award-of-central-government-contracts> .
- 11.4 Suppliers fulfilling this contract will be expected to complete a '[Social Value for Commercial Success](#)' - an e-learning course accessed through the Government Commercial College that can be found via the 'Social Value Mandatory eLearning' link. It takes less than one hour to complete and will help you to better understand what social value is, why it is important and how to implement it. It is expected that the successful supplier will complete this course at no additional cost to the Buyer.

11. PRICE

- 11.1 The contract will be awarded on a time and material basis using the suppliers agreed pricing structure via the G cloud 14 Framework agreement based on the 3 month (12 weeks discovery phase) followed by the 3 month reporting outputs and updates required.

12. STAFF AND CUSTOMER SERVICE

- 12.1 The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.
- 12.2 The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.
- 12.3 The Supplier shall ensure that staff understand the Buyer's vision and objectives and will provide excellent customer service to the Buyer throughout the duration of the Contract.
- 12.4 [REDACTED]

OFFICIAL

13. SECURITY AND CONFIDENTIALITY REQUIREMENTS

- 13.1 All of the Suppliers staff working on the requirement would need to be vetted to an SC level and would be asked to sign a confidentiality agreement as part of the contract.

14. PAYMENT AND INVOICING

- 14.1 Invoicing will be after each milestone above is satisfactorily completed.
- 14.2 Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.
- 14.3 Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.
- 14.4 Invoices should be submitted via email to: [REDACTED]

15. CONTRACT MANAGEMENT

- 15.1 The contract manager for this contract [REDACTED]
- 15.2 Meetings on progress are to be held virtually via Google meet on a monthly basis for the life of the contract.
- 15.3 There will be a final meeting prior to the end of the contract which will review performance against the deliverables set out above.
- 15.4 Attendance at Contract Review meetings shall be at the Supplier's own expense

16. INTELLECTUAL PROPERTY RIGHTS

- 16.1 Where the supplier is asked to develop any material specifically for the buyer, the intellectual property rights in that material shall be vested in the buyer, not the supplier.
- 16.2 Where the supplier is using material they have developed previously, the intellectual property rights will remain vested in the supplier, not the buyer.

17. LOCATION

- 17.1 The location of the Services will be carried out remotely and potentially at various UKSV offices including: [REDACTED] as required. The supplier should ensure all charges are included in the pricing for any travel requirements.

OFFICIAL



UBDS
DIGITAL
A UBDS GROUP COMPANY

UBDS DIGITAL PRICING

For G-Cloud 14

03 May 2024

Classification: Public

1 SKILLS FOR THE INFORMATION AGE (SFIA) DEFINITIONS AND RATE CARD

1.1 Please note that all pricing is based upon the SFIA rate card.

1.2 Standard Rate Card

	Strategy and architecture	Change and Transformation	Development and implementation	Delivery and Operation	People and skills	Relationships and engagement
Follow	£595	£595	£595	£595	£595	£595
Assist	£685	£685	£685	£685	£685	£685
Apply	£795	£795	£795	£795	£795	£795
Enable	£885	£885	£885	£885	£885	£885
Ensure or advise	£975	£975	£975	£975	£975	£975
Initiate or influence	£1195	£1195	£1195	£1195	£1195	£1195
Set strategy or inspire	£1350	£1350	£1350	£1350	£1350	£1350

Standards for consultancy day rate cards

- **Consultant's working day:** 8 hours exclusive of travel and lunch.
- **Working week:** Monday to Friday excluding national holidays.
- **Office hours:** 9:00am to 5:00pm Monday to Friday.
- **Travel, mileage subsistence:** Included in day rate within M25. Payable at department's standard travel and subsistence rates outside M25.
- **Mileage:** As for travel, mileage subsistence.
- Professional indemnity insurance: included in day rate.

1.3 Level Definitions

	Autonomy	Influence	Complexity	Business skills	Knowledge
Follow	Works under close direction. Uses little discretion in attending to enquiries. Is expected to seek guidance in unexpected situations.	Minimal Influence. May work alone or interact with immediate colleagues.	Performs routine activities in a structured environment. Requires assistance in resolving unexpected problems. Participates in the generation of new ideas.	<ul style="list-style-type: none"> ▪ Has sufficient oral and written communication skills for effective engagement with immediate colleagues. ▪ Uses basic systems and tools, applications and processes. ▪ Demonstrates an organised approach to work. Has basic digital skills to learn and use applications and tools for their role. ▪ Learning and professional development — contributes to identifying own development opportunities. ▪ Security, privacy and ethics — understands and complies with organisational standards. 	Has a basic generic knowledge appropriate to area of work. Applies newly acquired knowledge to develop new skills.

	Autonomy	Influence	Complexity	Business skills	Knowledge
Assist	Works under routine direction. Uses limited discretion in resolving issues or enquiries. Determines when to seek guidance in unexpected situations. Plans own work within short time horizons.	Interacts with and may influence immediate colleagues. May have some external contact with customers, suppliers and partners. Aware of need to collaborate with team and represent users/customer needs..	Performs a range of work activities in varied environments. May contribute to routine issue resolution. May apply creative thinking or suggest new ways to approach a task.	<ul style="list-style-type: none"> Has sufficient oral and written communication skills for effective engagement with colleagues and internal users/customers. Understands and uses appropriate methods, tools, applications and processes. Demonstrates a rational and organised approach to work. Has sufficient digital skills for their role. Learning and professional development — identifies and negotiates own development opportunities. Security, privacy and ethics — is fully aware of organisational standards. Uses appropriate working practices in own work. 	Has gained a basic domain knowledge. Demonstrates application of essential generic knowledge typically found in industry bodies of knowledge. Absorbs new information when it is presented systematically and applies it effectively
Apply	Works under general direction. Receives specific direction, accepts guidance and has work reviewed at agreed milestones. Uses discretion in identifying and responding to	Interacts with and influences colleagues. May oversee others or make decisions which impact routine work assigned to individuals or stages of projects. Has working level contact with customers,	Performs a range of work, sometimes complex and nonroutine, in a variety of environments. Applies a methodical approach to routine and moderately complex issue definition and	<ul style="list-style-type: none"> Demonstrates effective oral and written communication skills when engaging on issues with colleagues, users/ customers, suppliers and partners. Understands and effectively applies appropriate methods, tools, applications and processes. 	Has sound generic, domain and specialist knowledge necessary to perform effectively in the organisation typically gained from recognised bodies of knowledge and organisational information. Has an

	Autonomy	Influence	Complexity	Business skills	Knowledge
	complex issues related to own assignments. Determines when issues should be escalated to a higher level. Plans and monitors own work (and that of others where applicable) competently within limited deadlines.	suppliers and partners. Understands and collaborates on the analysis of user/customer needs and represents this in their work. Contributes fully to the work of teams by appreciating how own role relates to other roles.	resolution. Applies and contributes to creative thinking or finds new ways to complete tasks.	<ul style="list-style-type: none"> ▪ Demonstrates judgement and a systematic approach to work. ▪ Effectively applies digital skills and explores these capabilities for their role. ▪ Learning and professional development — takes the initiative to develop own knowledge and skills by identifying and negotiating appropriate development opportunities. ▪ Security, privacy and ethics — demonstrates appropriate working practices and knowledge in non-routine work. ▪ Appreciates how own role and others support appropriate working practices. 	appreciation of the wider business context. Demonstrates effective application and the ability to impart knowledge found in industry bodies of knowledge. Absorbs new information and applies it effectively
Enable	Works under general direction within a clear framework of accountability. Exercises substantial personal responsibility and autonomy. Uses substantial discretion in identifying and	Influences customers, suppliers and partners at account level. Makes decisions which influence the success of projects and team objectives. May have some responsibility for the work of others and for the allocation	Work includes a broad range of complex technical or professional activities, in a variety of contexts. Investigates, defines and resolves complex issues. Applies, facilitates and develops creative thinking concepts or	<ul style="list-style-type: none"> ▪ Communicates fluently, orally and in writing, and can present complex information to both technical and non-technical audiences when engaging with colleagues, users/customers, suppliers and partners. ▪ Selects appropriately from, and assesses the impact of change to applicable standards, methods, tools, applications 	Has a thorough understanding of recognised generic industry bodies of knowledge and specialist bodies of knowledge as necessary. Has gained a thorough knowledge of the domain of the organisation. Is able to

	Autonomy	Influence	Complexity	Business skills	Knowledge
	responding to complex issues and assignments as they relate to the deliverable/scope of work. Escalates when issues fall outside their framework of accountability. Plans, schedules and monitors work to meet given objectives and processes to time and quality targets.	of resources. Engages with and contributes to the work of cross-functional teams to ensure that customers and user needs are being met throughout the deliverable/scope of work. Facilitates collaboration between stakeholders who share common objectives. Participates in external activities related to own specialism.	finds innovative ways to approach a deliverable	<p>and processes relevant to own specialism.</p> <ul style="list-style-type: none"> ▪ Demonstrates an awareness of risk and takes an analytical approach to work ▪ Maximises the capabilities of applications for their role and evaluates and supports the use of new technologies and digital tools. ▪ Contributes specialist expertise to requirements definition in support of proposals. ▪ Shares knowledge and experience in own specialism to help others. ▪ Learning and professional development — maintains an awareness of developing practices and their application and takes responsibility for driving own development. Takes the initiative in identifying and negotiating their own and supporting team members' appropriate development opportunities. ▪ Contributes to the development of others. ▪ Security, privacy and ethics — fully understands the 	apply the knowledge effectively in unfamiliar situations and actively maintains own knowledge and shares with others. Rapidly absorbs and critically assesses new information and applies it effectively

	Autonomy	Influence	Complexity	Business skills	Knowledge
				importance and application to own work and the operation of the organisation. <ul style="list-style-type: none"> Engages or works with specialists as necessary 	
Ensure, advise	Works under broad direction. Work is often self-initiated. Is fully responsible for meeting allocated technical and/or group objectives. Analyses, designs, plans, executes and evaluates work to time, cost and quality targets. Establishes milestones and has a significant role in the assignment of tasks and/or responsibilities.	Influences organisation, customers, suppliers, partners and peers on the contribution of own specialism. Makes decisions which impact the success of assigned work, i.e. results, deadlines and budget. Has significant influence over the allocation and management of resources appropriate to given assignments. Leads on user/customer and group collaboration throughout all stages of work. Ensures users' needs are met consistently through each work stage. Builds appropriate	Implements and executes policies aligned to strategic plans. Performs an extensive range and variety of complex technical and/or professional work activities. Undertakes work which requires the application of fundamental principles in a wide and often unpredictable range of contexts. Engages and coordinates with subject matter experts to resolve complex issues as they relate to customer/organisational requirements. Understands the relationships between own specialism and customer/organisation	<ul style="list-style-type: none"> Demonstrates leadership in operational management. Analyses requirements and advises on scope and options for continual operational improvement. Assesses and evaluates risk. Takes all requirements into account when making proposals. Shares own knowledge and experience and encourages learning and growth. Advises on available standards, methods, tools, applications and processes relevant to group specialism(s) and can make appropriate choices from alternatives. Understands and evaluates the organisational impact of new technologies and digital services. Creatively applies innovative thinking and design practices in identifying solutions that will 	Is fully familiar with recognised industry bodies of knowledge both generic and specific, and knowledge of the business, suppliers, partners, competitors and clients. Develops a wider breadth of knowledge across the industry or business. Applies knowledge to help to define the standards which others will apply

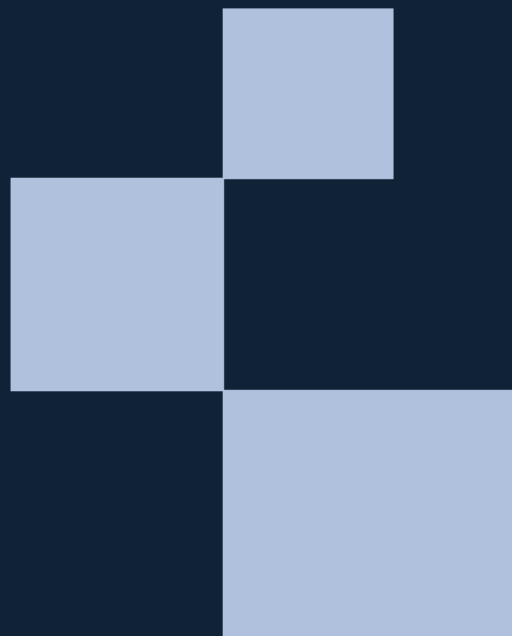
	Autonomy	Influence	Complexity	Business skills	Knowledge
		and effective business relationships across the organisation and with customers, suppliers and partners. Creates and supports collaborative ways of working across group/area of responsibility. Facilitates collaboration between stakeholders who have diverse objectives.	al requirements.	<p>deliver value for the benefit of the customer/stakeholder.</p> <ul style="list-style-type: none"> Clearly demonstrates impactful communication skills (oral, written and presentation) in both formal and informal settings, articulating complex ideas to broad audiences. Learning and professional development — takes initiative to advance own skills and identify and manage development opportunities in area of responsibility. Security, privacy and ethics — proactively contributes to the implementation of appropriate working practices and culture. 	
Initiate, influence	Has defined authority and accountability for actions and decisions within a significant area of work, including technical, financial and quality aspects. Establishes organisational objectives and assigns	Influences policy and strategy formation. Initiates influential relationships with internal and external customers, suppliers and partners at senior management level, including industry leaders. Leads on collaboration with a diverse range of stakeholders across	Contributes to the development and implementation of policy and strategy. Performs highly complex work activities covering technical, financial and quality aspects. Has deep expertise in own specialism(s) and an understanding of its impact on the broader	<ul style="list-style-type: none"> Demonstrates leadership in organisational management. Understands and communicates industry developments, and the role and impact of technology. Manages and mitigates organisational risk. Balances the requirements of proposals with the broader needs of the organisation. Promotes a learning and growth culture in their area of 	Has developed business knowledge of the activities and practices of own organisation and those of suppliers, partners, competitors and clients. Promotes the application of generic and specific bodies of knowledge in own organisation. Develops executive leadership

	Autonomy	Influence	Complexity	Business skills	Knowledge
	responsibilities.	competing objectives within the organisation. Makes decisions which impact the achievement of organisational objectives and financial performance.	business and wider customer/ organisation.	accountability. <ul style="list-style-type: none"> ▪ Leads on compliance with relevant legislation and the need for services, products and working practices to provide equal access and equal opportunity to people with diverse abilities. ▪ Identifies and endorses opportunities to adopt new technologies and digital services. ▪ Creatively applies a wide range of innovative and/or management principles to realise business benefits aligned to the organisational strategy. ▪ Communicates authoritatively at all levels across the organisation to both technical and non-technical audiences articulating business objectives. ▪ Learning and professional development — takes the initiative to advance own skills and leads the development of skills required in their area of accountability. ▪ Security, privacy and ethics — 	skills and broadens and deepens their industry or business knowledge.

	Autonomy	Influence	Complexity	Business skills	Knowledge
				takes a leading role in promoting and ensuring appropriate working practices and culture throughout own area of accountability and collectively in the organisation.	
Set Strategy, inspire, mobilise	At the highest organisational level, has authority over all aspects of a significant area of work, including policy formation and application. Is fully accountable for actions taken and decisions made, both by self and others to whom responsibilities have been assigned.	Inspires the organisation, and influences developments within the industry at the highest levels. Makes decisions critical to organisational success. Develops long-term strategic relationships with customers, partners, industry leaders and government. Collaborates with leadership stakeholders ensuring alignment to corporate vision and strategy.	Applies the highest level of leadership to the formulation and implementation of strategy. Performs extensive strategic leadership in delivering business value through vision, governance and executive management. Has a deep understanding of the industry and the implications of emerging technologies for the wider business environment.	<ul style="list-style-type: none"> Has a full range of strategic management and leadership skills. Communicates the potential impact of emerging practices and technologies on organisations and individuals and assesses the risks of using or not using such practices and technologies. Establishes governance to address business risk. Ensures proposals align with the strategic direction of the organisation. Fosters a learning and growth culture across the organisation. Assess the impact of legislation and actively promotes compliance and inclusivity. Advances the knowledge and/or exploitation of technology within one or more organisations. Champions creativity and 	Has established a broad and deep business knowledge including the activities and practices of own organisation and a broad knowledge of those of suppliers, partners, competitors and clients. Fosters a culture to encourage the strategic application of generic and specific bodies of knowledge within their own area of influence.

	Autonomy	Influence	Complexity	Business skills	Knowledge
				<p>innovation in driving strategy development to enable business opportunities.</p> <ul style="list-style-type: none">▪ Communicates persuasively and convincingly across own organisation, industry and government to audiences at all levels.▪ Learning and professional development — ensures that the organisation develops and mobilises the full range of required skills and capabilities.▪ Security, privacy and ethics — provides clear direction and strategic leadership for the implementation of working practices and culture throughout the organisation.	

**EXCEPTIONAL OUTCOMES.
NEVER COMPROMISE.**



Schedule 10 (Security Management: (Developer)

1 Buyer Options

Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements relating to that option set out in the relevant Paragraph:

Buyer risk assessment (see Paragraph 2)		
The Buyer has assessed this Agreement as:	a higher-risk agreement	<input checked="" type="checkbox"/>
	a standard agreement	<input type="checkbox"/>
Certifications (see Paragraph 8) (applicable only for standard risk agreements)		
Where the Buyer has assessed this Agreement as a standard risk agreement, the Supplier must have the following Certifications:	Cyber Essentials Plus	<input type="checkbox"/>
	Cyber Essentials	<input type="checkbox"/>
Locations (see Paragraph 1 of the Security Requirements)		
The Supplier and Sub-contractors may store, access or Process Government Data in:	the United Kingdom only	<input checked="" type="checkbox"/>
	the United Kingdom and European Economic Area only	<input type="checkbox"/>
	anywhere in the world not prohibited by the Buyer	<input type="checkbox"/>
Support Locations (see Paragraph 1 of the Security Requirements)		
The Supplier and Subcontractors may operate Support Locations in:	the United Kingdom only	<input checked="" type="checkbox"/>
	the United Kingdom and European Economic Area only	<input type="checkbox"/>
	anywhere in the world not prohibited by the Buyer	<input type="checkbox"/>

2 Buyer risk assessment

2.1 Where the Buyer has assessed this Agreement as a higher-risk agreement, the Supplier must:

- (a) comply with all requirements of this Schedule 10 (*Security Management*); and
- (b) hold the ISO/IEC 27001:2013 Relevant Certification from a UKAS-approved certification body (see Paragraph 8).

2.2 Where the Buyer has assessed this Agreement as a standard risk agreement, the Supplier must comply with all requirements of this this Schedule 10 (*Security Management*) except:

- (a) Paragraph 9 (*Security Management Plan*);
- (b) paragraph 9 of the Security Requirements (*Code Reviews*);

-
- (c) paragraph 11 of the Security Requirements (*Third-party Software Modules*);
 - (d) paragraph 12 of the Security Requirements (*Hardware and software support*);
 - (e) paragraph 13 of the Security Requirements (*Encryption*); and
 - (f) paragraph 19 of the Security Requirements (*Access Control*).

2.3 Where the Buyer has not made an assessment in the table in Paragraph 1, the Parties must treat this Agreement as a higher-risk agreement.

3 Definitions

3.1 In this Schedule 10 (*Security Management*):

“Anti-virus Software”	means software that: <ul style="list-style-type: none">protects the Supplier Information Management System from the possible introduction of Malicious Software;scans for and identifies possible Malicious Software in the Supplier Information Management System;if Malicious Software is detected in the Supplier Information Management System, so far as possible:<ul style="list-style-type: none">prevents the harmful effects of the Malicious Software; andremoves the Malicious Software from the Supplier Information Management System;
“Breach Action Plan”	means a plan prepared under paragraph 22.3 of the Security Requirements addressing any Breach of Security;
“Breach of Security”	means the occurrence of:

	<p>any unauthorised access to or use of the Services, the Buyer Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement, including the Buyer Data and the Code;</p> <p>the loss (physical or otherwise), corruption and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement, including the Buyer Data and the Code; and/or</p> <p>any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements;</p> <p>the installation of Malicious Software in the:</p> <p style="padding-left: 40px;">Supplier Information Management System;</p> <p style="padding-left: 40px;">Development Environment; or</p> <p style="padding-left: 40px;">Developed System;</p> <p>any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the:</p> <p style="padding-left: 40px;">Supplier Information Management System;</p> <p style="padding-left: 40px;">Development Environment; or</p> <p style="padding-left: 40px;">Developed System; and</p> <p>includes any attempt to undertake the activities listed in sub-paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:</p> <p style="padding-left: 40px;">was part of a wider effort to access information and communications technology by or on behalf of Central Government Bodies; or</p> <p style="padding-left: 40px;">was undertaken, or directed by, a state other than the United Kingdom</p>
“Buyer Data”	<p>means any:</p> <p style="padding-left: 40px;">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;</p> <p style="padding-left: 40px;">Personal Data for which the Buyer is a, or the, Data Controller; or</p> <p style="padding-left: 40px;">any meta-data relating to categories of data referred to in paragraphs (a) or (b);</p> <p>that is:</p> <p style="padding-left: 40px;">supplied to the Supplier by or on behalf of the Buyer; or</p>

	<p>that the Supplier generates, processes, stores or transmits under this Agreement; and</p> <p>for the avoidance of doubt includes the Code and any meta-data relating to the Code.</p>
“Buyer Data Register”	means the register of all Buyer Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer, produced and maintained in accordance with paragraph 23 of the Security Requirements;
“Buyer Equipment”	means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System;
“Buyer System”	means the information and communications technology system used by the Buyer to interface with the Supplier Information Management System or through which the Buyer receives the Services;
“Certification Default”	means the occurrence of one or more of the circumstances listed in Paragraph 8.4;
“Certification Rectification Plan”	means the plan referred to in Paragraph 8.5(a);
“Certification Requirements”	means the requirements set out in paragraph 8.3.
“CHECK Scheme”	means the NCSC’s scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks
“CHECK Service Provider”	<p>means a company which, under the CHECK Scheme:</p> <ul style="list-style-type: none"> has been certified by the National Cyber Security Centre; holds “Green Light” status; and is authorised to provide the IT Health Check services required by paragraph 18 of the Security Requirements;
“Code”	<p>means, in respect of the Developed System:</p> <ul style="list-style-type: none"> the source code; the object code; third-party components, including third-party coding frameworks and libraries; and all supporting documentation.
“Code Review”	<p>means a periodic review of the Code by manual or automated means to:</p> <ul style="list-style-type: none"> identify and fix any bugs; and ensure the Code complies with: <ul style="list-style-type: none"> the requirements of this Schedule 10 (<i>Security Management</i>); and the Secure Development Guidance;

“Code Review Plan”	means the document agreed with the Buyer under paragraph 9.3 of the Security Requirements setting out the requirements for, and frequency of, Code Reviews;
“Code Review Report”	means a report setting out the findings of a Code Review;
“Cyber Essentials”	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;
“Cyber Essentials Plus”	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
“Cyber Essentials Scheme”	means the Cyber Essentials scheme operated by the National Cyber Security Centre;
“Developed System”	means the software or system that the Supplier will develop under this Agreement;
“Development Activity”	means any activity relating to the development, deployment maintenance and upgrading of the Developed System, including: coding; testing; code storage; and deployment.
“Development Environment”	means any information and communications technology system and the Sites that the Supplier or its Sub-contractors will use to provide the Development Activity;
“EEA”	means the European Economic Area;
“End-user Device”	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services.
“Email Service”	means a service that will send, or can be used to send, emails from the Buyer’s email address or otherwise on behalf of the Buyer;
“HMG Baseline Personnel Security Standard”	means the employment controls applied to any individual member of the Supplier Personnel that performs any activity relating to the provision or management of the Services, as set out in “HMG Baseline Personnel Standard”, Version 6.0, May 2018 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf), as that document is updated from time to time;
“IT Health Check”	means security testing of the Supplier Information Management System, insofar as it relates to the Developed System but excluding the Development Environment in accordance with paragraph 33 of the Security Requirements;
“Malicious Software”	means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files,

	data or other information, executable code, applications, macros or configurations;
“Modules Register”	means the register of Third-party Software Modules required for higher risk agreements by paragraph 11.3 of the Security Requirements;
“NCSC”	means the National Cyber Security Centre;
“NCSC Cloud Security Principles”	means the NCSC’s document “Implementing the Cloud Security Principles” as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles .
“NCSC Device Guidance”	means the NCSC’s document “Device Security Guidance”, as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance ;
“NCSC Protecting Bulk Personal Data Guidance”	means the NCSC’s document “Protecting Bulk Personal Data”, as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data
“NCSC Secure Design Principles”	means the NCSC’s document “Secure Design Principles”, as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cyber-security-design-principles .
“OWASP”	means the Open Web Application Security Project Foundation;
“OWASP Secure Coding Practice”	means the Secure Coding Practices Quick Reference Guide published by OWASP, as updated or replaced from time to time and found at https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/migrated_content ;
“OWASP Top Ten”	means the list of the most critical security risks to web applications published annually by OWASP and found at https://owasp.org/www-project-top-ten/ ;
“Privileged User”	means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges;
“Process”	means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data;
“Prohibited Activity”	means the storage, access or Processing of Buyer Data prohibited by a Prohibition Notice;
“Prohibition Notice”	means a notice issued under paragraph 1.8 of the Security Requirements.
“Protective Monitoring System”	means the system implemented by the Supplier and its Sub-contractors under paragraph 20.1 of the Security Requirements to monitor and analyse access to and use of the Supplier Information Management System, the Development Environment, the Buyer Data and the Code

“Register of Support Locations and Third-Party Tools”	<p>means the part of the Security Management Plan setting out, in respect of Support Locations and Third-Party Tools:</p> <p>the nature of the activity performed at the Support Location or by the Third-Party Tool on the Code or the Buyer Data (as applicable);</p> <p>where that activity is performed by individuals, the place or facility from where that activity is performed; and</p> <p>in respect of the entity providing the Support Locations or Third-Party Tools, its:</p> <p>full legal name;</p> <p>trading name (if any)</p> <p>country of registration;</p> <p>registration number (if applicable); and</p> <p>registered address.</p>
“Relevant Activities”	means those activities specified in paragraph 0 of the Security Requirements.
“Relevant Certifications”	<p>means</p> <p>in the case of a standard agreement:</p> <p>Cyber Essentials; and/or</p> <p>Cyber Essentials Plus</p> <p>as determined by the Buyer; or</p> <p>in the case of a higher risk agreement:</p> <p>ISO/IEC 27001:2013 by a UKAS-approved certification body in respect of the Supplier Information Management System, or the Supplier Information Management System is included within the scope of a wider certification of compliance with ISO/IEC 27001:2013; and</p> <p>Cyber Essentials Plus;</p>
“Relevant Convictions”	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), or any other offences relevant to Services as the Buyer may specify
“Remediation Action Plan”	means the plan prepared by the Supplier in accordance with Paragraph 18.11 to 18.15, addressing the vulnerabilities and findings in a IT Health Check report
“Secure Development Guidance”	<p>means:</p> <p>the NCSC’s document “Secure development and deployment guidance” as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/developers-collection; and</p>

	the OWASP Secure Coding Practice as updated or replaced from time to time;
“Security Management Plan”	means the document prepared in accordance with the requirements of Paragraph 9 and in the format, and containing the information, specified in Annex 2.
“SMP Sub-contractor”	means a Sub-contractor with significant market power, such that: they will not contract other than on their own contractual terms; and either: there are no other substitutable suppliers of the particular services other than SMP Sub-contractors; or the Sub-contractor concerned has an effective monopoly on the provision of the Services.
“Sites”	means any premises: from or at which: the Services are (or are to be) provided; or the Supplier manages, organises or otherwise directs the provision or the use of the Services; or where: any part of the Supplier Information Management System is situated; or any physical interface with the Buyer System takes place; and for the avoidance of doubt include any premises at which Development Activities take place
“Sub-contractor”	includes, for the purposes of this Schedule 10 (<i>Security Management</i>), any individual or entity that: forms part of the supply chain of the Supplier; and has access to, hosts, or performs any operation on or in respect of the Supplier Information Management System, the Development Environment, the Code and the Buyer Data;
“Sub-contractor Personnel”	means: any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and engaged in or likely to be engaged in: the performance or management of the Services; or the provision of facilities or services that are necessary for the provision of the Services.
“Supplier Information”	means:

Management System	those parts of the information and communications technology system and the Sites that the Supplier or its Sub-contractors will use to provide the Services; the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources); and for the avoidance of doubt includes the Development Environment.
“Security Requirements”	mean the security requirements in Annex 1 to this Schedule 10 (<i>Security Management</i>)
“Supplier Personnel”	means any individual engaged, directly or indirectly, or employed by the Supplier or any Sub-contractor in the management or performance of the Supplier’s obligations under this Agreement;
“Support Location”	means a place or facility where or from which individuals may access or Process the Code or the Buyer Data;
“Support Register”	means the register of all hardware and software used to provide the Services produced and maintained for Higher Risk Agreements in accordance with paragraph 12 of the Security Requirements.
“Third-party Software Module”	means any module, library or framework that: is not produced by the Supplier or a Sub-contractor as part of the Development Activity; and either: forms, or will form, part of the Code; or is, or will be, accessed by the Developed System during its operation.
“Third-party Tool”	means any activity conducted other than by the Supplier during which the Code or the Buyer Data is accessed, analysed or modified or some form of operation is performed on it;
“UKAS”	means the United Kingdom Accreditation Service;

4 Introduction

4.1 This Schedule 10 (*Security Management*) sets out:

- (a) the assessment of this Agreement as either a:
 - (i) higher risk agreement; or
 - (ii) standard agreement,

in Paragraph 1;

-
- (b) the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Agreement to ensure the security of:
 - (i) the Development Activity;
 - (ii) the Development Environment;
 - (iii) the Buyer Data;
 - (iv) the Services; and
 - (v) the Supplier Information Management System;
 - (c) the principle of co-operation between the Supplier and the Buyer on security matters, in Paragraph 5;
 - (d) the Buyer's access to the Supplier Personnel and Supplier Information Management System, in Paragraph 7;
 - (e) the Certification Requirements, in Paragraph 8;
 - (f) the requirements for a Security Management Plan in the case of higher-risk agreements, in Paragraph 9; and
 - (g) the Security Requirements with which the Supplier and its Sub-contractors must comply.

5 Principles of Security

- 5.1 The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Buyer Data, and the integrity and availability of the Developed System, and, consequently, on the security of:
 - (a) the Sites;
 - (b) the Services; and
 - (c) the Supplier's Information Management System.
- 5.2 The Parties shall share information and act in a co-operative manner at all times to further the principles of security in Paragraph 5.1.
- 5.3 Notwithstanding the involvement of the Buyer in the assurance of the Supplier Information Management System, the Supplier remains responsible for:
 - (a) the security, confidentiality, integrity and availability of the Buyer Data when that Buyer Data is under the control of the Supplier or any of its Sub-contractors;
 - (b) the security and integrity of the Developed System; and
 - (c) the security of the Supplier Information Management System.
- 5.4 Where the Supplier, a Sub-contractor or any of the Supplier Personnel is granted access to the Buyer System or to the Buyer Equipment, it must comply with and ensure that all such Sub-contractors and Supplier Personnel comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Buyer System or the Buyer Equipment.

6 Security Requirements

6.1 The Supplier shall:

- (a) comply with the Security Requirements; and
- (b) subject to Paragraph 6.2, ensure that all Sub-contractors also comply with the Security Requirements.

6.2 Where a Sub-contractor is SMP Sub-contractor, the Supplier shall:

- (a) use best endeavours to ensure that the SMP Sub-contractor complies with the Security Requirements;
- (b) document the differences between Security Requirements the obligations that the SMP Sub-contractor is prepared to accept in sufficient detail to allow the Buyer to form an informed view of the risks concerned;
- (c) take such steps as the Buyer may require to mitigate those risks.

7 Access to Supplier Personnel and Supplier Information Management System

7.1 The Buyer may require, and the Supplier must provide, and ensure that each Sub-contractor provides, the Buyer and its authorised representatives with:

- (a) access to the Supplier Personnel, including, for the avoidance of doubt, the Sub-contractor Personnel;
- (b) access to the Supplier Information Management System, including those parts of the Supplier Information Management System under the control of, or operated by, any Sub-contractor; and
- (c) such other information and/or documentation that the Buyer or its authorised representatives may require,

to allow the Buyer to audit the Supplier and its Sub-contractors' compliance with this Schedule 10 (*Security Management*) and the Security Requirements.

7.2 The Supplier must provide the access required by the Buyer in accordance with Paragraph 7.1:

- (a) in the case of a Breach of Security within 24 hours of such a request; and
- (b) in all other cases, within 10 Working Days of such request.

8 Certification Requirements

8.1 The Supplier shall ensure that, unless otherwise agreed by the Buyer, both:

- (a) it; and
- (b) any Sub-contractor,

is certified as compliant with the Relevant Certifications.

-
- 8.2 Unless otherwise agreed by the Buyer, before it begins to provide the Services, the Supplier must provide the Buyer with a copy of:
- (a) the Relevant Certifications for it and any Sub-contractor; and
 - (b) in the case of a higher-risk agreement, any relevant scope and statement of applicability required under the ISO/IEC 27001:2013 Relevant Certifications.
- 8.3 The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications for it and any Sub-contractor are:
- (a) currently in effect;
 - (b) cover at least the full scope of the Supplier Information Management System; and
 - (c) are not subject to any condition that may impact the provision of the Services or the Development Activity (the “**Certification Requirements**”).
- 8.4 The Supplier must notify the Buyer promptly, and in any event within three (3) Working Days, after becoming aware that, in respect of it or any Sub-contractor:
- (a) a Relevant Certification has been revoked or cancelled by the body that awarded it;
 - (b) a Relevant Certification expired and has not been renewed by the Supplier;
 - (c) a Relevant Certification no longer applies to the full scope of the Supplier Information Management System; or
 - (d) the body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a “**Certification Default**”).
- 8.5 Where the Supplier has notified the Buyer of a Certification Default under Paragraph 8.4:
- (a) the Supplier must, within 10 Working Days of the date in which the Supplier provided notice under Paragraph 8.4 (or such other period as the Parties may agree) provide a draft plan (a “**Certification Rectification Plan**”) to the Buyer setting out:
 - (i) full details of the Certification Default, including a root cause analysis;
 - (ii) the actual and anticipated effects of the Certification Default;
 - (iii) the steps the Supplier and any Sub-contractor to which the Certification Default relates will take to remedy the Certification Default;
 - (b) the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;
 - (c) if the Buyer rejects the Certification Rectification Plan, the Supplier must within 5 Working Days of the date of the rejection submit a revised Certification Rectification Plan and Paragraph (b) will apply to the re-submitted plan;
 - (d) the rejection by the Buyer of a revised Certification Rectification Plan is a material Default of this Agreement;
 - (e) if the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

9 Security Management Plan

- 9.1 This Paragraph 9 applies only where the Buyer has assessed that this Agreement is a higher-risk agreement.

Preparation of Security Management Plan

- 9.2 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Schedule 10 (*Security Management*) and the Agreement in order to ensure the security of the Development Environment, the Developed System, the Buyer Data and the Supplier Information Management System.
- 9.3 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Agreement, the Security Management Plan, which must include:
- (a) an assessment of the Supplier Information Management System against the requirements of this Schedule 10 (*Security Management*), including the Security Requirements;
 - (b) the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Development Environment, the Developed System, the Buyer Data, the Buyer, the Services and/or users of the Services; and
 - (c) the following information, so far as is applicable, in respect of each Sub-contractor:
 - (i) the Sub-contractor's:
 - (A) legal name;
 - (B) trading name (if any);
 - (C) registration details (where the Sub-contractor is not an individual);
 - (ii) the Relevant Certifications held by the Sub-contractor;
 - (iii) the Sites used by the Sub-contractor;
 - (iv) the Development Activity undertaken by the Sub-contractor;
 - (v) the access the Sub-contractor has to the Development Environment;
 - (vi) the Buyer Data Processed by the Sub-contractor;
 - (vii) the Processing that the Sub-contractor will undertake in respect of the Buyer Data;
 - (viii) the measures the Sub-contractor has in place to comply with the requirements of this Schedule 10 (*Security Management*);
 - (d) the Register of Support Locations and Third Party Tools;
 - (e) the Modules Register;
 - (f) the Support Register;
 - (g) details of the steps taken to comply with:
 - (i) the Secure Development Guidance; and

-
- (ii) the secure development policy required by the ISO/IEC 27001:2013 Relevant Certifications;
 - (h) details of the protective monitoring that the Supplier will undertake in accordance with paragraph 20 of the Security Requirements, including:
 - (i) the additional audit and monitoring the Supplier will undertake of the Supplier Information Management System and the Development environment; and
 - (ii) the retention periods for audit records and event logs.

Approval of Security Management Plan

- 9.4 The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and must issue the Supplier with either:
- (a) an information security approval statement, which shall confirm that the Supplier may use the Supplier Information Management System to:
 - (i) undertake the Development Activity; and/or
 - (ii) Process Buyer Data; or
 - (b) a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.
- 9.5 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within 10 Working Days of the date of the rejection, or such other period agreed with the Buyer.
- 9.6 The rejection by the Buyer of a revised Security Management Plan is a material Default of this Agreement.

Updating Security Management Plan

- 9.7 The Supplier shall regularly review and update the Security Management Plan, and provide such to the Buyer, at least once each year and as required by this Paragraph.

Monitoring

- 9.8 The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:
- (a) a significant change to the components or architecture of the Supplier Information Management System;
 - (b) a new risk to the components or architecture of the Supplier Information Management System;
 - (c) a vulnerability to the components or architecture of the Supplier Information Management System using an industry standard vulnerability scoring mechanism;
 - (d) a change in the threat profile;
 - (e) a significant change to any risk component;
 - (f) a significant change in the quantity of Personal Data held within the Service;

-
- (g) a proposal to change any of the Sites from which any part of the Services are provided; and/or
 - (h) an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

9.9 Within 10 Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Security Management Plan and submit the updated Security Management Plan to the Buyer for review and approval.

Annex 1 Security Requirements

1 Location

Location for Relevant Activities

1.1 Unless otherwise agreed with the Buyer, the Supplier must, and ensure that its Sub-contractors, at all times:

- (a) undertake the Development Activity;
- (b) host the Development Environment; and
- (c) store, access or process Buyer Data,

(the “**Relevant Activities**”) only in the geographic areas permitted by the Buyer.

1.2 Where the Buyer has permitted the Supplier and its Sub-contractors to perform the Relevant Activities outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Sub-contractors undertake the Relevant Activities in a facility operated by an entity where:

- (a) the entity has entered into a binding agreement with the Supplier or Sub-contractor (as applicable);
- (b) that binding agreement includes obligations on the entity in relation to security management at least as onerous as those relating to Sub-contractors in this Schedule 5 (*Security Management*);
- (c) the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;
- (d) the Supplier has provided the Buyer with such information as the Buyer requires concerning:
 - (i) the entity;
 - (ii) the arrangements with the entity; and
 - (iii) the entity’s compliance with the binding agreement; and
- (e) the Buyer has not given the Supplier a Prohibition Notice under paragraph 1.8.

1.3 Where the Supplier cannot comply with one or more of the requirements of paragraph 1.2:

- (a) it must provide the Buyer with such information as the Buyer requests concerning:
 - (i) the security controls in places at the relevant location or locations; and
 - (ii) where certain security controls are not, or only partially, implemented the reasons for this;
- (b) the Buyer may grant approval to use that location or those locations, and that approval may include conditions; and

-
- (c) if the Buyer does not grant permission to use that location or those locations, the Supplier must, within such period as the Buyer may specify:
 - (i) cease to store, access or process Buyer Data at that location or those locations;
 - (ii) sanitise, in accordance with instructions from the Buyer, such equipment within the information and communications technology system used to store, access or process Buyer Data at that location, or those locations, as the Buyer may specify.

Support Locations

- 1.4 The Supplier must ensure that all Support Locations are located only in the geographic areas permitted by the Buyer.
- 1.5 Where the Buyer has permitted the Supplier and its Sub-contractors to operate Support Locations outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Sub-contractors operate the Support Locations in a facility operated by an entity where:
 - (a) the entity has entered into a binding agreement with the Supplier or Sub-contractor (as applicable);
 - (b) that binding agreement includes obligations on the entity in relation to security management at least as onerous as those relating to Sub-contractors in this Schedule 5 (*Security Management*);
 - (c) the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;
 - (d) the Supplier has provided the Authority with such information as the Authority requires concerning:
 - (i) the entity;
 - (ii) the arrangements with the entity; and
 - (iii) the entity's compliance with the binding agreement; and
 - (e) the Authority has not given the Supplier notice under paragraph 1.8.

Third-party Tools

- 1.6 The Supplier must use, and ensure that Sub-contractors use, only those Third-party Tools included in the Register of Support Locations and Third-party Tools.
- 1.7 The Supplier must not, and must not allow Sub-contractors to, use a new Third-party Tool, or replace an existing Third-party Tool, without the permission of the Buyer.

Prohibited Activities

- 1.8 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Sub-contractors must not undertake or permit to be undertaken some or all of the Relevant Activities or operate Support Locations (a "**Prohibited Activity**").
 - (a) in any particular country or group of countries;
 - (b) in or using facilities operated by any particular entity or group of entities; or

-
- (c) in or using any particular facility or group of facilities, whether operated by the Supplier, a Sub-contractor or a third-party entity,

(a “Prohibition Notice”).

- 1.9 Where the Supplier or Sub-contractor, on the date of the Prohibition Notice undertakes any Prohibited Activities affected by the notice, the Supplier must, and must procure that Sub-contractors, cease to undertake that Prohibited Activity within 40 Working Days of the date of the Prohibition Notice.

2 Vetting, Training and Staff Access

Vetting before performing or managing Services

- 2.1 The Supplier must not engage Supplier Personnel, and must ensure that Sub-contractors do not engage Sub-contractor Personnel in:

- (a) Development Activity;
- (b) any activity that provides access to the Development Environment; or
- (c) any activity relating to the performance and management of the Services

unless:

- (d) that individual has passed the security checks listed in paragraph 2.2; or
- (e) the Buyer has given prior written permission for a named individual to perform a specific role.

- 2.2 For the purposes of paragraph 2.1, the security checks are:

- (a) the checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:
 - (i) the individual’s identity;
 - (ii) the individual’s nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;
 - (iii) the individual’s previous employment history; and
 - (iv) that the individual has no Relevant Convictions;
- (b) national security vetting clearance to the level specified by the Buyer for such individuals or such roles as the Buyer may specify; or
- (c) such other checks for the Supplier Personnel of Sub-contractors as the Buyer may specify.

Annual training

- 2.3 The Supplier must ensure, and ensure that Sub-contractors ensure, that all Supplier Personnel, complete and pass security training at least once every calendar year that covers:

- (a) General training concerning security and data handling; and
- (b) Phishing, including the dangers from ransomware and other malware.

Staff access

- 2.4 The Supplier must ensure, and ensure that Sub-contractors ensure, that individual Supplier Personnel can access only the Buyer Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.
- 2.5 The Supplier must ensure, and ensure that Sub-contractors ensure, that where individual Supplier Personnel no longer require access to the Buyer Data or any part of the Buyer Data, their access to the Buyer Data or that part of the Buyer Data is revoked immediately when their requirement to access Buyer Data ceases.
- 2.6 Where requested by the Buyer, the Supplier must remove, and must ensure that Sub-contractors remove, an individual Supplier Personnel's access to the Buyer Data, or part of that Buyer Data specified by the Buyer, as soon as practicable and in any event within 24 hours of the request.

Exception for certain Sub-contractors

- 2.7 Where the Supplier considers it cannot ensure that a Sub-contractors will undertake the relevant security checks on any Sub-contractor Personnel, it must:
 - (a) as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;
 - (b) provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Sub-contractor Personnel will perform as the Buyer reasonably requires; and
 - (c) comply, at the Supplier's cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Personnel and the management of the Sub-contractor.

3 End-user Devices

- 3.1 The Supplier must manage, and must ensure that all Sub-contractors manage, all End-user Devices on which Buyer Data or Code is stored or processed in accordance with the following requirements:
 - (a) the operating system and any applications that store, process or have access to Buyer Data or Code must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;
 - (b) users must authenticate before gaining access;
 - (c) all Buyer Data and Code must be encrypted using a encryption tool agreed to by the Buyer;
 - (d) the End-user Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;
 - (e) the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Buyer Data and Code to ensure the security of that Buyer Data and Code;
 - (f) the Supplier or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Buyer Data or Code stored on the device and prevent any user or group of users from accessing the device;
 - (g) all End-user Devices are within the scope of any Relevant Certification.

3.2 The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Agreement.

3.3 Where there is any conflict between the requirements of this Schedule 10 (*Security Management*) and the requirements of the NCSC Device Guidance, the requirements of this Schedule take precedence.

4 **Secure Architecture**

4.1 The Supplier shall design and build the Developed System in a manner consistent with:

- (a) the NCSC's guidance on "Security Design Principles for Digital Services";
- (b) where the Developed System will Process bulk data, the NCSC's guidance on "Bulk Data Principles"; and
- (c) the NCSC's guidance on "Cloud Security Principles".

4.2 Where any of the documents referred to in paragraph 4.1 provides for various options, the Supplier must document the option it has chosen to implement and its reasons for doing so.

5 **Secure Software Development by Design**

5.1 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity, implement secure development and deployment practices to ensure that:

- (a) no malicious code is introduced into the Developed System or the Supplier Information Management System.
- (b) the Developed System can continue to function in accordance with the Specification:
 - (i) in unforeseen circumstances; and
 - (ii) notwithstanding any attack on the Developed System using common cyber-attack techniques, including attacks using those vulnerabilities identified at any time in the OWASP Top Ten.

5.2 To those ends, the Supplier must, and ensure that all Sub-contractors engaged in Development Activity:

- (a) comply with the Secure Development Guidance as if its requirements were terms of this Contract; and
- (b) document the steps taken to comply with that guidance as part of the Security Management Plan.

5.3 In particular, the Supplier must, and ensure that all Sub-contractors engaged in Development Activity:

- (a) ensure that all Supplier Staff engaged in Development Activity are:
 - (i) trained and experienced in secure by design code development;
 - (ii) provided with regular training in secure software development and deployment;

-
- (b) ensure that all Code:
 - (i) is subject to a clear, well-organised, logical and documented architecture;
 - (ii) follows OWASP Secure Coding Practice
 - (iii) follows recognised secure coding standard, where one is available;
 - (iv) employs consistent naming conventions;
 - (v) is coded in a consistent manner and style;
 - (vi) is clearly and adequately documented to set out the function of each section of code;
 - (vii) is subject to appropriate levels of review through automated and non-automated methods both as part of:
 - (A) any original coding; and
 - (B) at any time the Code is changed;
 - (c) ensure that all Development Environments:
 - (i) protect access credentials and secret keys;
 - (ii) are logically separate from all other environments, including production systems, operated by the Supplier or Sub-contractor;
 - (iii) require multi-factor authentication to access;
 - (iv) have onward technical controls to protect the Developed System or the Supplier Information Management System in the event a Development Environment is compromised;
 - (v) use network architecture controls to constrain access from the Development Environment to the Developed System or the Supplier Information Management System;

6 Code Repository and Deployment Pipeline

- 7 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity:
 - 7.1 when using a cloud-based code depository for the deployment pipeline, use only a cloud-based code depository that has been assessed against the NCSC Cloud Security Principles;
 - 7.2 ensure user access to code repositories is authenticated using credentials, with passwords or private keys;
 - 7.3 ensure secret credentials are separated from source code.
 - 7.4 run automatic security testing as part of any deployment of the Developed System.

8 Development and Testing Data

- 8.1 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity, use only anonymised, dummy or synthetic data when using data within the Development Environment for the purposes of development and testing, .

9 Code Reviews

- 9.1 This paragraph applies where the Buyer has assessed that this Agreement is a higher-risk agreement.
- 9.2 The Supplier must:
- (a) regularly; or
 - (b) as required by the Buyer
- review the Code in accordance with the requirements of this paragraph 9 (a “**Code Review**”).
- 9.3 Before conducting any Code Review, the Supplier must agree with the Buyer:
- (a) the modules or elements of the Code subject to the Code Review;
 - (b) the development state at which the Code Review will take place;
 - (c) any specific security vulnerabilities the Code Review will assess; and
 - (d) the frequency of any Code Reviews (the “**Code Review Plan**”).
- 9.4 For the avoidance of doubt, the Code Review Plan may specify different modules or elements of the Code are reviewed at a different development state, for different security vulnerabilities and at different frequencies.
- 9.5 The Supplier:
- (a) must undertake Code Reviews in accordance with the Code Review Plan; and
 - (b) may undertake Code Reviews by automated means if this is consistent with the approach specified in the Code review Plan.
- 9.6 No later than 10 Working Days or each Code Review, the Supplier must provide the Buyer with a full, unedited and unredacted copy of the Code Review Report.
- 9.7 Where the Code Review identifies any security vulnerabilities, the Supplier must:
- (a) remedy these at its own cost and expense;
 - (b) ensure, so far as reasonably practicable, that the identified security vulnerabilities are not present in any other modules or code elements; and
 - (c) modify its approach to undertaking the Development Activities to ensure, so far as is practicable, the identified security vulnerabilities will not re-occur; and
 - (d) provide the Buyer with such information as it requests about the steps the Supplier takes under this paragraph 9.7.

10 Third-party Software

- 10.1 The Supplier must not, and must ensure that Sub-contractors do not, use any software to Process Buyer Data where the licence terms of that software purport to grant the licensor rights to Process the Buyer Data greater than those rights strictly necessary for the use of the software.

11 Third-party Software Modules

- 11.1 This paragraph 11 applies only where the Buyer has assessed that this Agreement is a higher-risk agreement
- 11.2 Where the Supplier or a Sub-contractor incorporates a Third-party Software Module into the Code, the Supplier must:
- (a) verify the source and integrity of the Third-party Software Module by cryptographic signing or such other measure that provides the same level of assurance;
 - (b) perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that Third-party Software Module;
 - (c) continue to monitor any such Third-party Software Module so as to ensure it promptly becomes aware of any newly-discovered security vulnerabilities;
 - (d) take appropriate steps to minimise the effect of any such security vulnerability on the Developed System.
- 11.3 The Supplier must produce and maintain a register of all Third-party Software Modules that form part of the Code (the **"Modules Register"**).
- 11.4 The Modules Register must include, in respect of each Third-party Software Module:
- (a) full details of the developer of the module;
 - (b) the due diligence the Supplier undertook on the Third-party Software Module before deciding to use it;
 - (c) any recognised security vulnerabilities in the Third-party Software Module; and
 - (d) how the Supplier will minimise the effect of any such security vulnerability on the Developed System.
- 11.5 The Supplier must:
- (a) review and update the Modules Register:
 - (i) within 10 Working Days of becoming aware of a security vulnerability in any Third-party Software Module; and
 - (ii) at least once every 6 (six) months;
 - (b) provide the Buyer with a copy of the Modules Register:
 - (i) whenever it updates the Modules Register; and
 - (ii) otherwise when the Buyer requests.

12 Hardware and software support

- 12.1 This paragraph 12 applies only where the Buyer has assessed that this Agreement is a higher-risk agreement
- 12.2 The Supplier must ensure that all software used to provide the Services remains at all times in full security support, including any extended or bespoke security support.
- 12.3 The Supplier must produce and maintain a register of all software that form the Supplier Information Management System (the “**Support Register**”).
- 12.4 The Support Register must include in respect of each item of software:
- (a) the date, so far as it is known, that the item will cease to be in mainstream security support; and
 - (b) the Supplier’s plans to upgrade the item before it ceases to be in mainstream security support.
- 12.5 The Supplier must:
- (a) review and update the Support Register:
 - (i) within 10 Working Days of becoming aware of the date on which, or any change to the date on which, any item of software will cease to be in mainstream security report;
 - (ii) within 10 Working Days of introducing new software, or removing existing software, from the Supplier Information Management System; and
 - (iii) at least once every 12 (twelve) months;
 - (b) provide the Buyer with a copy of the Support Register:
 - (i) whenever it updates the Support Register; and
 - (ii) otherwise when the Buyer requests.
- 12.6 Where any element of the Developed System consists of COTS Software, the Supplier shall ensure:
- (a) those elements are always in mainstream or extended security support from the relevant vendor; and
 - (b) the COTS Software is not more than one version or major release behind the latest version of the software.
- 12.7 The Supplier shall ensure that all hardware used to provide the Services, whether used by the Supplier or any Sub-contractor is, at all times, remains in mainstream vendor support, that is, that in respect of the hardware, the vendor continues to provide:
- (a) regular firmware updates to the hardware; and
 - (b) a physical repair or replacement service for the hardware.

13 Encryption

- 13.1 This paragraph applies where the Buyer has assessed that this Agreement is a higher-risk agreement.
- 13.2 Before Processing any Buyer Data, the Supplier must agree with the Buyer the encryption methods that it and any Sub-contractors that Process Buyer Data will use to comply with this paragraph 13.
- 13.3 Where this paragraph 13 requires Buyer Data to be encrypted, the Supplier must use, and ensure that Subcontractors use, the methods agreed by the Buyer under paragraph 13.2.
- 13.4 Notwithstanding anything in the specification for the Developed System or this Agreement, the Supplier must ensure that the Developed System encrypts Buyer Data:
- (a) when the Buyer Data is stored at any time when no operation is being performed on it; and
 - (b) when the buyer Data is transmitted.
- 13.5 Unless paragraph 13.6 applies, the Supplier must ensure, and must ensure that all Sub-contractors ensure, that Buyer Data is encrypted:
- (a) when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and
 - (b) when transmitted.
- 13.6 Where the Supplier, or a Sub-contractor, cannot encrypt Buyer Data as required by paragraph 13.5, the Supplier must:
- (a) immediately inform the Buyer of the subset or subsets of Buyer Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
 - (b) provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption;
 - (c) provide the Buyer with such information relating to the Buyer Data concerned, the reasons why that Buyer Data cannot be encrypted and the proposed protective measures as the Buyer may require.
- 13.7 The Buyer, the Supplier and, where the Buyer requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Buyer Data.
- 13.8 Where the Buyer and Supplier reach agreement, the Supplier must update the Security Management Plan to include:
- (a) the subset or subsets of Buyer Data not encrypted and the circumstances in which that will occur;
 - (b) the protective measure that the Supplier and/or Sub-contractor will put in place in respect of the unencrypted Buyer Data.
- 13.9 Where the Buyer and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Buyer Data, either party may refer the matter to the Technical Design Authority.

14 Email

- 14.1 Notwithstanding anything in the specification for the Developed System or this Agreement, the Supplier must ensure that where the Developed System will provide an Email Service to the Buyer, the Developed System:
- (a) supports transport layer security (“**TLS**”) version 1.2, or higher, for sending and receiving emails;
 - (b) supports TLS Reporting (“**TLS-RPT**”);
 - (c) is capable of implementing:
 - (i) domain-based message authentication, reporting and conformance (“**DMARC**”);
 - (ii) sender policy framework (“**SPF**”); and
 - (iii) domain keys identified mail (“**DKIM**”); and
 - (d) is capable of complying in all respects with any guidance concerning email security as issued or updated from time to time by:
 - (i) the UK Government (current version at <https://www.gov.uk/guidance/set-up-government-email-services-securely>); or
 - (ii) the NCSC (current version at <https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing>).

15 DNS

- 15.1 Unless otherwise agreed by the Buyer, the Supplier must ensure that the Developed System uses the UK public sector Protective DNS (“**PDNS**”) service to resolve internet DNS queries.

16 Malicious Software

- 16.1 The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier Information Management System.
- 16.2 The Supplier must ensure that such Anti-virus Software:
- (a) prevents the installation of the most common forms of Malicious Software in the Supplier Information Management System and the Development Environment;
 - (b) is configured to perform automatic software and definition updates;
 - (c) provides for all updates to be the Anti-virus Software to be deployed within 10 Working Days of the update’s release by the vendor;
 - (d) performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and
 - (e) where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.
- 16.3 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or

corruption of Buyer Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

- 16.4 The Supplier must at all times, during and after the Term, on written demand indemnify the Buyer and keep the Buyer indemnified, against all Losses incurred by, awarded against or agreed to be paid by the Buyer arising from any Breach of Security caused by Malicious Software where the Breach of Security arose from a failure by the Supplier, or a Sub-contractor, to comply with this paragraph .

17 Vulnerabilities

- 17.1 Unless the Buyer otherwise agrees, the Supplier must ensure that it or any relevant Sub-contractor applies security patches to any vulnerabilities in the Supplier Information Management System no later than:
- (a) seven (7) days after the public release of patches for vulnerabilities classified as “critical”;
 - (b) thirty (30) days after the public release of patches for vulnerabilities classified as “important”; and
 - (c) sixty (60) days after the public release of patches for vulnerabilities classified as “other”.
- 17.2 The Supplier must:
- (a) scan the Supplier Information Management System and the Development Environment at least once every month to identify any unpatched vulnerabilities; and
 - (b) if the scan identifies any unpatched vulnerabilities ensure they are patched in accordance with paragraph 17.1.
- 17.3 For the purposes of this paragraph 17, the Supplier must implement a method for classifying vulnerabilities to the Supplier Information Management System as “critical”, “important” or “other” that is aligned to recognised vulnerability assessment systems, such as:
- (a) the National Vulnerability Database’s vulnerability security ratings; or
 - (b) Microsoft’s security bulletin severity rating system.

18 Security testing

Responsibility for security testing

- 18.1 The Supplier is solely responsible for:
- (a) the costs of conducting any security testing required by this Paragraph 18 (unless the Buyer gives notice under Paragraph 18.2); and
 - (b) the costs of implementing any findings, or remedying any vulnerabilities, identified in that security testing.

Security tests by Buyer

- 18.2 The Buyer may give notice to the Supplier that the Buyer will undertake the security testing required by Paragraph 18.4(a) and 18.4(d).

18.3 Where the Buyer gives notice under Paragraph 18.2:

- (a) the Supplier shall provide such reasonable co-operation as the Buyer requests, including:
 - (i) such access to the Supplier Information Management System as the Buyer may request; and
 - (ii) such technical and other information relating to the Information Management System as the Buyer requests;
- (b) the Buyer must provide a full, unedited and unredacted copy of the report relating to the IT Health Check as soon as reasonably practicable after the Buyer receives a copy of the report; and
- (c) for the purposes of Paragraphs 18.8 to 18.17:
 - (i) the Supplier must treat any IT Health Check commissioned by the Buyer as if it were such a report commissioned by the Supplier; and
 - (ii) the time limits in Paragraphs 18.8 and 18.11 run from the date on which the Buyer provides the Supplier with the copy of the report under Paragraph (b).

Security tests by Supplier

18.4 The Supplier must:

- (a) during the testing of the Developed System and before the Developed System goes live (unless the Buyer gives notice under Paragraph 18.2);
- (b) at least once during each Contract Year; and
- (c) when required to do so by the Buyer;

undertake the following activities:

- (d) conduct security testing of the Developed System and the Supplier Information Management System, insofar as it relates to the Developed System but excluding the Development Environment (an “IT Health Check”) in accordance with Paragraph 18.5 to 18.7; and
- (e) implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph and 18.8 to 18.17.

IT Health Checks

18.5 In arranging an IT Health Check, the Supplier must:

- (a) use only a CHECK Service Provider to perform the IT Health Check;
- (b) design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier Information Management System and the delivery of the Services.
- (c) promptly provide the Buyer with such technical and other information relating to the Information Management System as the Buyer requests;
- (d) include within the scope of the IT Health Check such tests as the Buyer requires;
- (e) agree with the Buyer the scope, aim and timing of the IT Health Check.

-
- 18.6 The Supplier must commission the IT Health Check in accordance with the scope, aim and timing agreed by the Buyer.
- 18.7 Following completion of an IT Health Check, the Supplier must provide the Buyer with a full, unedited and unredacted copy of the report relating to the IT Health Check without delay and in any event within 10 Working Days of its receipt by the Supplier.

Remedying vulnerabilities

- 18.8 In addition to complying with Paragraphs 18.4 to 18.17, the Supplier must remedy:
- (a) any vulnerabilities classified as critical in the IT Health Check report within 5 Working Days of becoming aware of the vulnerability and its classification;
 - (b) any vulnerabilities classified as high in the IT Health Check report within 1 month of becoming aware of the vulnerability and its classification; and
 - (c) any vulnerabilities classified as medium in the IT Health Check report within 3 months of becoming aware of the vulnerability and its classification.
- 18.9 The Supplier must notify the Buyer immediately if it does not, or considers it will not be able to, remedy the vulnerabilities classified as critical, high or medium in the IT Health Check report within the time periods specified in Paragraph 18.8.

Significant vulnerabilities

- 18.10 Where the IT Health Check report identifies more than 10 vulnerabilities classified as either critical or high, the Buyer may, at the Supplier's cost, appoint an independent and appropriately qualified and experienced security architect and adviser to perform a root cause analysis of the identified vulnerabilities.

Responding to an IT Health Check report

- 18.11 Where the IT Health Check identifies vulnerabilities in, or makes findings in respect of, the Information Management System, the Supplier must within 20 Working Days of receiving the IT Health Check report, prepare and submit for approval to the Buyer a draft plan addressing the vulnerabilities and findings (the "**Remediation Action Plan**").
- 18.12 Where the Buyer has commissioned a root cause analysis under Paragraph 18.10, the Supplier shall ensure that the draft Remediation Action Plan addresses that analysis.
- 18.13 The draft Remediation Action Plan must, in respect of each vulnerability identified or finding made by the IT Health Check report:
- (a) how the vulnerability or finding will be remedied;
 - (b) the date by which the vulnerability or finding will be remedied; and
 - (c) the tests that the Supplier proposes to perform to confirm that the vulnerability has been remedied or the finding addressed.
- 18.14 The Supplier shall promptly provide the Buyer with such technical and other information relating to the Supplier Information Management System, the IT Health Check report or the draft Remediation Action Plan as the Buyer requests.

18.15 The Buyer may:

- (a) reject the draft Remediation Action Plan where it considers that the draft Remediation Action Plan is inadequate, providing its reasons for doing so, in which case:
 - (i) the Supplier shall within 10 Working Days of the date on which the Buyer rejected the draft Remediation Action Plan submit a revised draft Remediation Action Plan that takes into account the Buyer's reasons; and
 - (ii) paragraph 18.13 to 18.15 shall apply, with appropriate modifications, to the revised draft Remediation Action Plan;
- (b) accept the draft Remediation Action Plan, in which case the Supplier must immediately start work on implementing the Remediation Action Plan in accordance with Paragraph 18.16 and 18.17.

Implementing an approved Remediation Action Plan

- 18.16 In implementing the Remediation Action plan, the Supplier must conduct such further tests on the Supplier Information Management System as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has fully and correctly implemented.
- 18.17 If any such testing identifies a new risk, new threat, vulnerability or exploitation technique with the potential to affect the security of the Supplier Information Management System, the Supplier shall within 1 Working Day of becoming aware of such risk, threat, vulnerability or exploitation technique:
- (a) provide the Buyer with a full, unedited and unredacted copy of the test report;
 - (b) implement interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available;
 - (c) as far as practicable, remove or disable any extraneous interfaces, services or capabilities not needed for the provision of the Services within the timescales set out in the test report or such other timescales as may be agreed with the Buyer.

19 Access Control

19.1 This paragraph applies where the Buyer has assessed that this Agreement is a higher-risk agreement.

19.2 The Supplier must, and must ensure that all Sub-contractors:

- (a) identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;
- (b) require multi-factor authentication for all user accounts that have access to Buyer Data or that are Privileged Users;
- (c) allow access only to those parts of the Supplier Information Management System and Sites that those persons require;
- (d) maintain records detailing each person's access to the Supplier Information Management System and Sites, and make those records available to the Buyer on request.

-
- 19.3 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that the user accounts for Privileged Users of the Supplier Information Management System:
- (a) are allocated to a single, individual user;
 - (b) are accessible only from dedicated End-user Devices;
 - (c) are configured so that those accounts can only be used for system administration tasks;
 - (d) require passwords with high complexity that are changed regularly;
 - (e) automatically log the user out of the Supplier Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive; and
 - (f) in the case of a higher-risk agreement are:
 - (i) restricted to a single role or small number of roles;
 - (ii) time limited; and
 - (iii) restrict the Privileged User's access to the internet.
- 19.4 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that it logs all activity of the Privileged Users while those users access those accounts and keeps the activity logs for 20 Working Days before deletion.
- 19.5 The Supplier must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different high-complexity passwords for their different accounts on the Supplier Information Management System.
- 19.6 The Supplier must ensure that the Developed System is developed and configured so as to provide for the matters set out in paragraphs 19.2 to 19.5.
- 19.7 The Supplier must, and must ensure that all Sub-contractors:
- (a) configure any hardware that forms part of the Supplier Information Management System that is capable of requiring a password before it is accessed to require a password; and
 - (b) change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.

20 **Event logging and protective monitoring**

Protective Monitoring System

- 20.1 The Supplier must, and must ensure that Sub-contractors, implement an effective system of monitoring and reports analysing access to and use of the Supplier Information Management System, the Development Environment, the Buyer Data and the Code to:
- (a) identify and prevent potential Breaches of Security;
 - (b) respond effectively and in a timely manner to Breaches of Security that do occur;
 - (c) identify and implement changes to the Supplier Information Management System to prevent future Breaches of Security; and

-
- (d) help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier Information Management System or the Developed System

(the “**Protective Monitoring System**”).

20.2 The Protective Monitoring System must provide for:

- (a) event logs and audit records of access to the Supplier Information Management system; and
- (b) regular reports and alerts to identify:
 - (i) changing access trends;
 - (ii) unusual usage patterns; or
 - (iii) the access of greater than usual volumes of Buyer Data;
- (c) the detection and prevention of any attack on the Supplier Information Management System or the Development Environment using common cyber-attack techniques;
- (d) any other matters required by the Security Management Plan.

Event logs

20.3 The Supplier must ensure that, unless the Buyer otherwise agrees, any event logs do not log:

- (a) personal data, other than identifiers relating to users; or
- (b) sensitive data, such as credentials or security keys.

Provision of information to Buyer

20.4 The Supplier must provide the Buyer on request with:

- (a) full details of the Protective Monitoring System it has implemented; and
- (b) copies of monitoring logs and reports prepared as part of the Protective Monitoring System.

Changes to Protective Monitoring System

20.5 The Buyer may at any time require the Supplier to update the Protective Monitoring System to:

- (a) respond to a specific threat identified by the Buyer;
- (b) implement additional audit and monitoring requirements; and
- (c) stream any specified event logs to the Buyer’s security information and event management system.

21 **Audit rights**

Right of audit

-
- 21.1 The Buyer may undertake an audit of the Supplier or any Sub-contractor to:
- (a) verify the Supplier's or Sub-contractor's (as applicable) compliance with the requirements of this Schedule 10 (*Security Management*) and the Data Protection Laws as they apply to Buyer Data;
 - (b) inspect the Supplier Information Management System (or any part of it);
 - (c) review the integrity, confidentiality and security of the Buyer Data; and/or
 - (d) review the integrity and security of the Code.
- 21.2 Any audit undertaken under this Paragraph 21:
- (a) may only take place during the Term and for a period of 18 months afterwards; and
 - (b) is in addition to any other rights of audit the Buyer has under this Agreement.
- 21.3 The Buyer may not undertake more than one audit under Paragraph 21.1 in each calendar year unless the Buyer has reasonable grounds for believing:
- (a) the Supplier or any Sub-contractor has not complied with its obligations under this Agreement or the Data Protection Laws as they apply to the Buyer Data;
 - (b) there has been or is likely to be a Security Breach affecting the Buyer Data or the Code; or
 - (c) where vulnerabilities, or potential vulnerabilities, in the Code have been identified by:
 - (i) an IT Health Check; or
 - (ii) a Breach of Security.

Conduct of audits

- 21.4 The Authority must use reasonable endeavours to provide 15 Working Days' notice of an audit.
- 21.5 The Authority must when conducting an audit:
- (a) comply with all relevant policies and guidelines of the Supplier or Sub-contractor (as applicable) concerning access to the Supplier Information Management System the Buyer considers reasonable having regard to the purpose of the audit; and
 - (b) use reasonable endeavours to ensure that the conduct of the audit does not unreasonably disrupt the Supplier or Sub-contractor (as applicable) or delay the provision of the Services.
- 21.6 The Supplier must, and must ensure that Sub-contractors, on demand provide the Buyer with all co-operation and assistance the Buyer may reasonably require, including:
- (a) all information requested by the Buyer within the scope of the audit;
 - (b) access to the Supplier Information Management System; and
 - (c) access to the Supplier Staff.

Response to audit findings

21.7 Where an audit finds that:

- (a) the Supplier or a Sub-contractor has not complied with this Agreement or the Data Protection Laws as they apply to the Buyer Data; or
- (b) there has been or is likely to be a Security Breach affecting the Buyer Data

the Buyer may require the Supplier to remedy those defaults at its own cost and expense and within the time reasonably specified by the Buyer.

21.8 The exercise by the Buyer of any rights it may have under this Paragraph 3 does not affect the exercise by it of any other or equivalent rights it may have under this Agreement in respect of the audit findings.

22 Breach of Security

Reporting Breach of Security

22.1 If either party becomes aware of a Breach of Security it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within 24 hours.

Immediate steps

22.2 The Supplier must, upon becoming aware of a Breach of Security immediately take those steps identified in the Security Management Plan (if applicable) and all other steps reasonably necessary to:

- (a) minimise the extent of actual or potential harm caused by such Breach of Security;
- (b) remedy such Breach of Security to the extent possible;
- (c) apply a tested mitigation against any such Breach of Security; and
- (d) prevent a further Breach of Security in the future which exploits the same root cause failure;

Subsequent action

22.3 As soon as reasonably practicable and, in any event, within 5 Working Days, or such other period agreed with the Buyer, following the Breach of Security, provide to the Buyer:

- (a) full details of the Breach of Security; and
- (b) if required by the Buyer:
 - (i) a root cause analysis; and
 - (ii) a draft plan addressing the root cause of the Breach of Security(the "**Breach Action Plan**").

22.4 The draft Breach Action Plan must, in respect of each issue identified in the root cause analysis:

- (a) how the issue will be remedied;
- (b) the date by which the issue will be remedied; and

-
- (c) the tests that the Supplier proposes to perform to confirm that the issue has been remedied or the finding addressed.
- 22.5 The Supplier shall promptly provide the Buyer with such technical and other information relating to the draft Breach Action Plan as the Buyer requests.
- 22.6 The Buyer may:
- (a) reject the draft Breach Action Plan where it considers that the draft Breach Action Plan is inadequate, providing its reasons for doing so, in which case:
 - (i) the Supplier shall within 10 Working Days of the date on which the Buyer rejected the draft Breach Action Plan submit a revised draft Breach Action Plan that takes into account the Buyer's reasons; and
 - (ii) paragraph 22.5 and 22.6 shall apply to the revised draft Breach Action Plan;
 - (b) accept the draft Breach Action Plan, in which case the Supplier must immediately start work on implementing the Breach Action Plan.

Assistance to Buyer

- 22.7 Where the Breach of Security concerns or is connected with the Buyer Data or the Code, the Supplier must provide such assistance to the Buyer as the Buyer requires until the Breach of Security and any impacts or potential impacts on the Buyer are resolved to the Buyer's satisfaction.
- 22.8 The obligation to provide assistance under Paragraph 22.7 continues notwithstanding the expiry or termination of this Contract.

Reporting of Breach of Security to regulator

- 22.9 Where the Law requires the Supplier report a Breach of Security to the appropriate regulator, the Supplier must:
- (a) make that report within the time limits:
 - (i) specified by the relevant regulator; or
 - (ii) otherwise required by Law;
 - (b) to the extent that the relevant regulator or the Law permits, provide the Buyer with a full, unredacted and unedited copy of that report at the same time it is sent to the relevant regulator.
- 22.10 Where the Law requires the Buyer to report a Breach of Security to the appropriate regulator, the Supplier must:
- (a) provide such information and other input as the Buyer requires within the timescales specified by the Buyer;
 - (b) where Paragraph 7 applies to the Breach of Security, ensure so far as practicable the report it sends to the relevant regulator is consistent with the report provided by the Buyer.

23 Return and Deletion of Buyer Data

23.1 The Supplier must create and maintain a register of:

- (a) all Buyer Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer; and
- (b) those parts of the Supplier Information Management System, including those parts of the Supplier Information Management System that are operated or controlled by any Sub-contractor, on which the Buyer Data is stored (the "**Buyer Data Register**").

23.2 The Supplier must:

- (a) review and update the Buyer Data Register:
 - (i) within 10 Working Days of the Supplier or any Sub-contractor changes to those parts of the Supplier Information Management System on which the Buyer Data is stored;
 - (ii) within 10 Working Days of a significant change in the volume, nature or overall sensitivity of the Buyer Data stored on the Supplier Information Management System;
 - (iii) at least once every 12 (twelve) months; and
- (b) provide the Buyer with a copy of the Buyer Data Register:
 - (i) whenever it updates the Buyer Data Register; and
 - (ii) otherwise when the Buyer requests.

23.3 The Supplier must, and must ensure that all Sub-contractors, securely erase any or all Buyer Data held by the Supplier or Sub-contractor, including any or all Code:

- (a) when requested to do so by the Buyer; and
- (b) using a deletion method agreed with the Buyer that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.

23.4 The Supplier must, and must ensure that all Sub-contractors, provide the Buyer with copies of any or all Buyer Data held by the Supplier or Sub-contractor, including any or all Code:

- (a) when requested to do so by the Buyer; and
- (b) using the method specified by the Buyer.

Annex 2 Security Management Plan

[Insert Security Management Plan]