

# G-Cloud 13 Call-Off Contract

This Call-Off Contract for the G-Cloud 13 Framework Agreement (RM1557.13) includes:

**G-Cloud 13 Call-Off Contract**

Part A: Order Form 2

Part B: Terms and conditions 15

Schedule 1: Services 36

Schedule 2: Call-Off Contract charges 37

Schedule 3: Collaboration agreement 38

Schedule 4: Alternative clauses 51

Schedule 5: Guarantee 56

Schedule 6: Glossary and interpretations 65

Schedule 7: UK GDPR Information 83

Annex 1: Processing Personal Data 84

Annex 2: Joint Controller Agreement 89

# 

# 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** | 184894260352817 |
| **Call-Off Contract reference** | CCIT22A33 |
| **Call-Off Contract title** | Provision of GovAssure Programme Part 2 |
| **Call-Off Contract description** | 1. Conduct assurance reviews for Home Office for up to three systems each. 2. Necessary;  * Experience of working within government * Hold a minimum of SC clearance * Have familiarity with cyber assessment frameworks including the NCSC CAF * Are CREST or NCSC qualified  1. Provide feedback to the programme team to help in honing the developed process for GovAssure. 2. Use the supplied self-assessment template to records their assessment of a department’s system 3. Participate in a lesson learnt workshops with programme stakeholders. 4. On completion of the contract, transfer all deliverables to the programme team with a clear handover package |
| **Start date** | Monday 13th February 2023 |
| **Expiry date** | Friday 12th May 2023 |
| **Call-Off Contract value** | Initial Contract Value £52,000.00 ex VAT  Total Contract Value including extension period £104,000.00 ex VAT |
| **Charging method** | BACS |
| **Purchase order number** | To be confirmed upon commencement of  agreement |

This Order Form is issued under the G-Cloud 13 Framework Agreement (RM1557.13).

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  **REDACTED TEXT under FOIA Section 40, Personal Information**. |
| **To the Supplier** | NCC Group Security Services Limited  **REDACTED TEXT under FOIA Section 40, Personal Information**. |
| **Together the ‘Parties’** | |

### Principal contact details

**For the Buyer:**

Title: **REDACTED TEXT under FOIA Section 40, Personal Information**.

Name: **REDACTED TEXT under FOIA Section 40, Personal Information**.

Email: **REDACTED TEXT under FOIA Section 40, Personal Information**.

**For the Supplier:**

Title: **REDACTED TEXT under FOIA Section 40, Personal Information**.

Name: **REDACTED TEXT under FOIA Section 40, Personal Information**.

Email: **REDACTED TEXT under FOIA Section 40, Personal Information**.

Phone: **REDACTED TEXT under FOIA Section 40, Personal Information**.

### Call-Off Contract term

|  |  |
| --- | --- |
| **Start date** | This Call-Off Contract Starts on **13th February 2023** and is **valid for three (3) months** |
| **Ending**  **(termination)** | The notice period for the Supplier needed for Ending the Call-Off Contract is at least **30** Working Days from the date of written notice for undisputed sums (as per clause 18.6).  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). |
| **Extension period** | This Call-Off Contract can be extended by the Buyer **for one**  **period of up to 3 months**, **by giving the Supplier 4 weeks written notice b**efore its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.  Extensions which extend the Term beyond 36 months are  only permitted if the Supplier complies with the additional exit  plan requirements at clauses 21.3 to 21.8.  If a buyer is a central government department and the  contract Term is intended to exceed 24 months, then under  the Spend Controls process, prior approval must be obtained  from the Government Digital Service (GDS). Further  guidance:  [https://www.gov.uk/service-manual/agile-delivery/spend-contr](https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service)  ols-check-if-you-need-approval-to-spend-money-on-a-service |

### 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** | This Call-Off Contract is for the provision of Services Under:   * Lot 3: Cloud support |
| **G-Cloud Services required** | The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below:   1. Conduct assurance reviews for two departments (Home Office) for up to three systems each. 2. Necessary;  * Experience of working within government * Hold a minimum of SC clearance * Have familiarity with cyber assessment frameworks including the NCSC CAF * Are CREST or NCSC qualified  1. Provide feedback to the programme team to help in honing the developed process for GovAssure. 2. Use the supplied self-assessment template to records their assessment of a department’s system 3. Participate in a lesson learnt workshops with programme stakeholders. 4. On completion of the contract transfer all deliverables to the programme team with a clear handover package |
| **Additional Services** | N/A |
| **Location** | The location of the Services will be carried out at an office in Whitehall in London (exact location will be agreed with the supplier) |
| **Quality Standards** | The quality standards required for this Call-Off Contract are;  **Staff security clearance - Conforms to BS7858:2019**  **Government security clearance -**   * Hold a minimum of SC clearance * **Up to Developed Vetting (DV)** |
| **Technical Standards:** | The technical standards used as a requirement for this Call-Off are;  **Service delivery lifecycle complies with NCSC and ISO 20700 Standards** |
| **Service level agreement:** | |  |  |  |  | | --- | --- | --- | --- | | **KPI/ SLA** | **Service Area** | **KPI/SLA description** | **Target** | | 1 | Duration of reviews | Suppliers will be expected to conduct a system assurance review within 5 days unless departments require more time | 5 days | | 2 | Results | Suppliers are expected to provide results from the assurance reviews with 5 days | 5 days | | 3 | Preparation | Suppliers are expected to agree to attend meeting to prepare for audit | Within 24 hours | | 4 | Training | Suppliers will agree to attend provided training session on how to conduct an assurance review | Within 24 hours | | 5 | Lessons learnt | Suppliers will agree to attend and provide data to aid in lesson learnt workshops | Within 24 hours | |
| **Onboarding** | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |

|  |  |
| --- | --- |
| **Offboarding** | **REDACTED TEXT under FOIA Section 43 Commercial Interests**. |
| **Collaboration agreement** | N/A |
| **Limit on Parties’ liability** | The annual total liability of either Party for all Property Defaults will not exceed 125%  The annual total liability for Buyer Data Defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.  The annual total liability 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 |
| **Insurance** | The Supplier insurance(s) required will be:   * **a minimum insurance period of 6 years** following the expiration or Ending of this Call-Off Contract. * **professional indemnity insurance** cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) * **employers' liability insurance** with a minimum limit of £5,000,000 or any higher minimum limit required by Law |
| **Buyer’s responsibilities** | N/A |
| **Buyer’s equipment** | N/A |

### Supplier’s information

|  |  |
| --- | --- |
| **Subcontractors or partners** | N/A |

### 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** | Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables |
| **Invoice details** | Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.  The supplier will indicate to the programme when milestones have been met to aid receipting. |
| **Who and where to send invoices to** | Invoices will be sent to:  **REDACTED TEXT under FOIA Section 40, Personal Information**.  **REDACTED TEXT under FOIA Section 40, Personal Information**.  **REDACTED TEXT under FOIA Section 40, Personal Information**.  We will send you a unique PO Number to **REDACTED TEXT under FOIA Section 40, Personal Information**.  once this agreement has been executed by both parties. You must be in  receipt of a valid PO Number before submitting an invoice.  To avoid delay in payment it is important that the invoice is compliant and  that it includes a valid PO number, and the details (name and telephone  number) of your Customer contact (i.e. Contract Manager), and also  what is being purchased.  Non-compliant invoices will be sent back to you, which may lead to a  delay in payment. If you have a query regarding an outstanding payment please contact our Accounts Payable section either by email to **REDACTED TEXT under FOIA Section 40, Personal Information**  or by telephone **REDACTED TEXT under FOIA Section 40, Personal Information** between 09:00-17:00 Monday to Friday. |
| **Invoice information required** | All invoices must include:   1. ● The Purchase Order number 2. ● Contract reference 3. ● Date 4. ● Address (Buyer and Supplier) 5. ● Supplier name and contact details 6. ● Remittance and payment bank account details 7. ● Description of the charges 8. ● Volume of the charges 9. ● Unit cost of the charges |
| **Invoice frequency** | The supplier will indicate to the programme when milestones have been met to aid receipting. |
| **Call-Off Contract value** | The total value of this Call-Off Contract £104,000.00 ex VAT |
| **Call-Off Contract charges** | **REDACTED TEXT under FOIA Section 43 Commercial Interests** |

### Additional Buyer terms

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Performance of the** **Service** | |  |  |  | | --- | --- | --- | | **Milestone/ Deliverable** | **Description** | **Timeframe or Delivery Date** | | 1 | Preparation for assurance reviews | Within week 1 of agreement on date with the dept/GSG | | 2 | Conduct assurance review | Within week 1 of agreement on date with the dept | | 3 | Submit results to GSG | Within week 1 of completion for a system | | 4 | Lessons learnt | Within week 1 of agreement on date with the dept | |
| **Guarantee** | N/A |
| **Warranties, representations** | In addition to the incorporated Framework Agreement clause 2.3, the Supplier warrants and represents to the Buyer that solutions provided to Cabinet Office will be defect free and the IPR will solely rest with Cabinet Office. |
| **Supplemental requirements in addition to the Call-Off** **terms** | Schedule 8 - Security Management |
| **Alternative clauses** | N/A |
| **Buyer specific**  **amendments**  **to/refinements of the Call-Off Contract terms** | N/A |
| **Personal Data and** **Data Subjects** | Annex 1 of Schedule 7 is being used. |
| **Intellectual Property** | N/A |
| **Social Value** | N/A |

### 

### 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 clause 8.3 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 RM1557.13 .

|  |  |  |
| --- | --- | --- |
| **Signed** | Supplier | Buyer |
| **Name** | **REDACTED TEXT under FOIA Section 40, Personal Information** | **REDACTED TEXT under FOIA Section 40, Personal Information** |
| **Title** | **REDACTED TEXT under FOIA Section 40, Personal Information** | **REDACTED TEXT under FOIA Section 40, Personal Information** |
| **Signature** | **REDACTED TEXT under FOIA Section 40, Personal Information** | **REDACTED TEXT under FOIA Section 40, Personal Information** |
| **Date** | **23/12/22** | **27/01/23** |

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

## Customer Benefits

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

[G-Cloud 13 Customer Benefit Record](https://crowncommercial.qualtrics.com/jfe/form/SV_9YO5ox0tT0ofQ0u)

# 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 24 months.

### 2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses 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)
* 10 (Force majeure)
* 5.3 (Continuing rights)
* 5.4 to 5.6 (Change of control)
* 5.7 (Fraud)
* 5.8 (Notice of fraud)
* 7 (Transparency and Audit)
* 8.3 (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)
* 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:

* + 1. a reference to the ‘Framework Agreement’ will be a reference to the ‘Call-Off Contract’
    2. a reference to ‘CCS’ or to ‘CCS and/or the Buyer’ will be a reference to ‘the Buyer’
    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
  1. 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. The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause ‘XX’, where ‘XX’ is the Framework Agreement clause number.
  3. 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

9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.

9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.

9.8 The Supplier will be liable for the payment of any:

9.8.1 premiums, which it will pay promptly

9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

### 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:

1. alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
2. alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;
3. 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:

* + 1. rights granted to the Buyer under this Call-Off Contract
    2. Supplier’s performance of the Services
    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:

* + 1. modify the relevant part of the Services without reducing its functionality or performance
    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
    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:

* + 1. the use of data supplied by the Buyer which the Supplier isn’t required to verify under this Call-Off Contract
    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-securityclassifications

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management[: https://www.cpni.gov.uk/content/adopt-risk-managementapproach](https://www.cpni.gov.uk/content/adopt-risk-management-approach) and Protection of Sensitive Information and Assets: <https://www.cpni.gov.uk/protection-sensitive-information-and-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](https://www.gov.uk/government/publications/technology-code-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/technology-code-of-practice/technology-code->

[of-practice](https://www.gov.uk/government/publications/technology-code-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[.](https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary)

### 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:

* + 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
    2. return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
    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
    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
    5. work with the Buyer on any ongoing work
    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
  1. 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.
  2. 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 GDS 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 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than 30 consecutive days, the other Party may End this Call-Off Contract with immediate effect by written notice.

### 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 isn’t 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

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.

* 1. 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.
  2. The Supplier will co-operate 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.
  3. The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:
     1. its failure to comply with the provisions of this clause
     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
  4. The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.
  5. 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 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. 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 CallOff 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.

# **Schedule 1: Services / Specification of Requirements**

1. **PURPOSE**
   1. Government Security Group are required to procure an external cyber security reviewer to conduct an assurance review of departments (Home Office) self-assessment against the Cyber Assessment Framework as part of the GovAssure pilots. GovAssure is a new cyber security assurance process for Government Departments. Government Security Group are paying for a company to conduct the review on the departments behalf as this was a prerequisite for the departments participating in the pilots.
2. **BACKGROUND TO THE CONTRACTING AUTHORITY**
   1. The Government Security Group is responsible for the oversight, coordination and delivery of protective security within all central government departments, their agencies and arms-length bodies.
   2. The Group oversees the Government Security Function and sets the strategy and standards for government security across people, physical and information/cyber and drawing upon expert advice from the National Cyber Security Centre and Centre for the Protection of National Infrastructure.
   3. GSG supports Ministers, the Cabinet Secretary and Chief Executive of the Civil Service by monitoring departmental security performance and managing serious or pan-government security risks and incidents.
3. **BACKGROUND TO REQUIREMENT / OVERVIEW OF REQUIREMENT**
   1. The programme is looking to deliver the first output from the Government Cybersecurity Strategy and this will be GovAssure. GovAssure is looking to implement a new assurance regime across HMG that will provide a cross government view of departmental cybersecurity postures.
   2. GovAssure differs from other assurance processes as it will incorporate not only a self-assessment of the departmental cyber postures but will also include a third-party assessment of the department to add rigour to the measurement against CAF.
   3. Once complete, a department will receive a “get well” report listing current vulnerabilities which will then allow it to spend its cyber budget more effectively and to mitigate specific risks quickly.
   4. We are in the pilot phase at the moment which will allow us to test and hone the developed process and to gain insights from stakeholders on our approach.
4. **DEFINITIONS**



1. **SCOPE OF REQUIREMENTS**
   1. What is in scope:
      1. Preparatory activities for assurance reviews
      2. Conducting assurance reviews
      3. To provide results back to GSG in a timely manner
      4. To provide feedback on what went well and what didn’t during reviews
      5. To participate in lesson learnt with the programme team
   2. What is excluded:
      1. To discuss or agree which systems need to be assessed
      2. To discuss or agree what profile the system will be measured against
      3. To provide non-data driven decisions or speculative recommendations on what a department show do to mitigate risk
2. **THE REQUIREMENT**
   1. During our pilot phase, the programme is looking to procure a set of suppliers to conduct assurance reviews for two departments (Home Office) for up to three systems each.
   2. In order to do this we are looking for suppliers that have:
      1. Experience of working within government
      2. Hold a minimum of SC clearance
      3. Have familiarity with cyber assessment frameworks including the NCSC CAF
      4. Are CREST or NCSC qualified
   3. During the contract, the supplier will be providing feedback to the programme team to help in honing the developed process for GovAssure.
   4. The Supplier will use the supplied self-assessment template to records their assessment of a department’s system
   5. The supplier will be expected to participate in lessons learnt workshops with programme stakeholders.
   6. The Supplier will on completion of the contract transfer all deliverables to the programme team with a clear handover package
3. **KEY MILESTONES AND DELIVERABLES** 
   1. The following Contract milestones/deliverables shall apply:

|  |  |  |
| --- | --- | --- |
| **Milestone/ Deliverable** | **Description** | **Timeframe or Delivery Date** |
| 1 | Preparation for assurance reviews | Within week 1 of agreement on date with the dept/GSG |
| 2 | Conduct assurance review | Within week 1 of agreement on date with the dept |
| 3 | Submit results to GSG | Within week 1 of completion for a system |
| 4 | Lessons learnt | Within week 1 of agreement on date with the dept |

1. **MANAGEMENT INFORMATION/REPORTING**
   1. The supplier is expected to use the provided self-assessment document to mark their observations and comments against individual
2. **VOLUMES**
   1. The suppliers are expected to conduct three (3) system assurance reviews per department.
3. **CONTINUOUS IMPROVEMENT**
   1. The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.
   2. The Supplier should present new ways of working to the Authority during monthly Contract review meetings.
   3. Changes to the way in which the Services are to be delivered must be brought to the Authority’s attention and agreed prior to any changes being implemented.
4. **QUALITY**
   1. Assurers will adhere to the standards set forth by the GovAssure programme for the duration of the contract.
5. **PRICE**
   1. The Contracting Authorities Budget is £52,000.00 excl. VAT for 3 Months. Total Contract value inclusive of the extension period is £104,000.00 excl. VAT.
   2. Pricing will be in accordance with the supplier’s G-Cloud pricing document.
6. **STAFF AND CUSTOMER SERVICE**
   1. The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.
   2. The Supplier’s staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.
   3. The Supplier shall ensure that staff understand the Authority’s vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.
7. **SERVICE LEVELS AND PERFORMANCE**

**REDACTED TEXT under FOIA Section 43 Commercial Interests**

1. **SECURITY AND CONFIDENTIALITY REQUIREMENTS**

**REDACTED TEXT under FOIA Section 43 Commercial Interests**

1. **PAYMENT AND INVOICING**

**REDACTED TEXT under FOIA Section 43 Commercial Interests**

1. **CONTRACT MANAGEMENT**

**REDACTED TEXT under FOIA Section 43 Commercial Interests**

1. **LOCATION**

**REDACTED TEXT under FOIA Section 43 Commercial Interests**

# **Schedule 2: Call-Off Contract charges**

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the

**REDACTED TEXT under FOIA Section 43 Commercial Interests**

Supplier’s Platform pricing document) can’t be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will include:

**Schedule 3: Collaboration agreement (not used in this agreement)**

**Collaboration Agreement Schedule 2 (not used in this agreement)**

**Schedule 4: Alternative clauses (not used in this agreement)**

**Schedule 5: Guarantee (not used in this agreement)**

#### 

## **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** | For each Party, IPRs:   * 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   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. |
| **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** | Data, Personal Data and any information, which may include (but isn’t limited to) any:   * 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** | Default is any:   * 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   Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a 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](https://www.gov.uk/guidance/check-employment-status-for-tax) |
| **Expiry Date** | The expiry date of this Call-Off Contract in the Order Form. |
| **Force Majeure** | A force Majeure event means anything affecting either Party's performance of their obligations arising from any:   * 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   The following do not constitute a Force Majeure event:   * 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 RM1557.13 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** | Can be:   * a voluntary arrangement * a winding-up petition * the appointment of a receiver or administrator * an unresolved statutory demand * a Schedule A1 moratorium * a Dun & Bradstreet rating of 10 or less |
| **Intellectual Property** **Rights or IPR** | Intellectual Property Rights are:   * 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 * 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 * all other rights having equivalent or similar effect in any country or jurisdiction |
| **Intermediary** | For the purposes of the IR35 rules an intermediary can be:   * the supplier's own limited company * a service or a personal service company or a partnership   It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency). |
| **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** | 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. |
| **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. |
| **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** | 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:   * 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: o 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 GCloud Services, including backup 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-controlsche ck-if-you-need-approval-to-spend-money-on-a-service](https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-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 GCloud 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. |
| **Variation** | This has the meaning given to it in clause 32 (Variation process). |
| **Working Days** | Any day other than a Saturday, Sunday or public holiday in England and Wales. |
| **Year** | A contract year. |

## **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. The contact details of the Buyer’s Data Protection Officer are: **REDACTED TEXT under FOIA Section 40, Personal Information**
  2. The contact details of the Supplier’s Data Protection Officer are: **REDACTED TEXT under FOIA Section 40, Personal Information**
  3. The Processor shall comply with any further written instructions with respect to Processing by the Controller.

* 1. Any such further instructions shall be incorporated into this Annex.

|  |  |
| --- | --- |
| **Descriptions** | **Details** |
| Identity of Controller for each Category of Personal Data | **The Buyer is Controller and the Supplier is Processor**  The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of of any personal data processed in  providing the services. |
| Duration of the Processing | The duration of the Call-Off Contract unless  terminated earlier or extended under Part A  ‘Call-Off Contract term’ above. |
| Nature and purposes of the Processing | The use of staff email addresses between the department, Cabinet Office and supplier |
| Type of Personal Data | Staff names and email addresses |
| Categories of Data Subject | Staff |
| Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data | Data and Information shall only be retained by  the processor for the duration of the contract  only plus the legally required period for retaining relevant records. |

### 

## **Annex 2: Joint Controller Agreement - (not used in this agreement)**

### 

20221111 Security Schedule for Consultancy v0.7 (10.11.2022)(112671518.8)

**Schedule 8 - Supplemental requirements in addition to the Call-Off terms** **: Security Management**

# **Buyer Options**

**Risk assessment**

|  |  |  |
| --- | --- | --- |
| The Buyer has assessed this Agreement as | a standard consultancy agreement | X |
| a higher-risk consultancy agreement | ☐ |

**Relevant Certifications**

|  |  |  |
| --- | --- | --- |
| Where the Buyer has assessed this Agreement as a standard consultancy agreement, it requires the Supplier to be certified as compliant with: | Cyber Essentials | ☐ |
| Cyber Essentials Plus | X |

# **Provider Cyber Essentials Certificates**

# **Supplier obligations**

## Where the Buyer has assessed this Agreement as a higher-risk consultancy agreement, the Supplier must comply with all requirements in this Schedule 8 (Security Management).

## Where the Buyer has assessed this Agreement as a standard consultancy agreement, the Supplier must comply with this Schedule 8 (Security Management), other than:

### the requirement to be certified as compliant with ISO/IEC 27001:2013 under Paragraph 7.1(b);

### the requirement to undertake security testing of the Supplier Information Management System in accordance with paragraph 3 of Appendix 1;

### the requirement to produce a Security Management Plan in accordance with Paragraph 8

### the requirement to document unencrypted Buyer Data in the Security Management Plan in accordance with paragraph 5.4 of Appendix 1

# **Definitions**

* 1. In this Schedule 8 (Security Management):

|  |  |
| --- | --- |
| * 1. “Anti-virus Software” | means software that:   * + 1. protects the Supplier Information Management System from the possible introduction of Malicious Software;     2. scans for and identifies possible Malicious Software in the Supplier Information Management System;     3. if Malicious Software is detected in the Supplier Information Management System, so far as possible:        1. prevents the harmful effects of the Malicious Software; and        2. removes the Malicious Software from the Supplier Information Management System. |
| * 1. “Breach of Security” | * 1. means the occurrence of:      1. 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 Subcontractor in connection with this Agreement;      2. the loss (physical or otherwise) and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Buyer, the Supplier or any Subcontractor in connection with this Agreement; and/or      3. any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements. |
| * 1. “Buyer Data” | * 1. means any:      1. 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; or      2. Personal Data for which the Buyer is a, or the, Data Controller,   2. that is:      + 1. supplied to the Supplier by or on behalf of the Buyer; or        2. that the Supplier generates, processes, stores or transmits under this Agreement. |
| * 1. “Buyer Equipment” | * 1. means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System. |
| * 1. “Buyer System” | * 1. 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. |
| * 1. “Certification Default” | * 1. means the occurrence of one or more of the circumstances listed in paragraph 7.4. |
| * 1. “Certification Rectification Plan” | * 1. means the plan referred to in paragraph 7.5(a). |
| * 1. “Certification Requirements” | * 1. means the information security requirements set out in paragraph 7. |
| * 1. “Cyber Essentials” | * 1. means the Cyber Essentials certificate issued under the Cyber Essentials Scheme. |
| * 1. “Cyber Essentials Plus” | * 1. means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme. |
| * 1. “Cyber Essentials Scheme” | * 1. means the Cyber Essentials scheme operated by the National Cyber Security Centre. |
| * 1. “End-user Device” | * 1. means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services. |
| * 1. “HMG Baseline Personnel Security Standard” | * 1. 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. |
| * 1. “Malicious Software” | * 1. 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. |
| * 1. “NCSC Cloud Security Principles” | * 1. means the National Cyber Security Centre’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. |
| * 1. “NCSC Device Guidance” | * 1. means the National Cyber Security Centre’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. |
| * 1. “Privileged User” | * 1. means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges. |
| * 1. “Process” | * 1. 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. |
| * 1. “Prohibited Activity” | * 1. means the storage, access or Processing of Buyer Data prohibited by a Prohibition Notice. |
| * 1. “Prohibition Notice” | * 1. means a notice issued under paragraph 1.3 of Appendix 1. |
| * 1. “Relevant Certifications” | * 1. means those certifications specified in paragraph 7.1. |
| * 1. “Relevant Convictions” | * 1. 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. |
| * 1. “Security Management Plan” | * 1. means the document prepared in accordance with the requirements of paragraph 8. |
| * 1. “Sites” | * 1. means any premises:      1. from or at which:         1. the Services are (or are to be) provided; or         2. the Supplier manages, organises or otherwise directs the provision or the use of the Services; or      2. where:         1. any part of the Supplier Information Management System is situated; or         2. any physical interface with the Buyer System takes place. |
| * 1. “Standard Contractual Clauses” | * 1. means the standard data protection clauses specified in Article 46 of the United Kingdom General Data Protection Regulation setting out the appropriate safeguards for the transmission of personal data outside the combined territories of the United Kingdom and the European Economic Area. |
| * 1. “Supplier Information Management System” | * 1. means:      1. those parts of the information and communications technology system and the Sites that the Supplier or its Subcontractors will use to provide the Services; and      2. the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources); |
| * 1. “Sub-contractor Personnel” | * 1. means:      1. any individual engaged, directly or indirectly, or employed, by any Subcontractor; and      2. engaged in or likely to be engaged in:         1. the performance or management of the Services;         2. or the provision of facilities or services that are necessary for the provision of the Services. |
| * 1. “Supplier Personnel” | * 1. means any individual engaged, directly or indirectly, or employed by the Supplier or any Subcontractor in the management or performance of the Supplier’s obligations under this Agreement. |
| * 1. “UKAS” | * 1. means the United Kingdom Accreditation Service. |

# **Introduction**

## This Schedule 8 (Security Management) sets out:

### 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 the Buyer Data, the Services and the Supplier Information Management System;

### the assessment of this Agreement as either a:

#### standard consultancy agreement; or

#### higher-risk consultancy agreement,

in paragraph 1;

### the Buyer’s access to the Supplier Personnel and Supplier Information Management System, in paragraph 6;

### the Certification Requirements, in paragraph 7;

### the requirements for a Security Management Plan in the case of higher-risk consultancy agreements, in paragraph 8; and

### the security requirements with which the Supplier and Sub-contractors must comply in Appendix 1.

# **Principles of security**

## The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Buyer Data and, consequently on the security of:

### the Sites;

### the Services; and

### the Supplier’s Information Management System.

## The Supplier is responsible for:

### 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 Subcontractors; and

### the security of the Supplier Information Management System.

## The Supplier:

### comply with the security requirements in Appendix 1; and

### ensure that each Subcontractor that Processes Buyer Data complies with the security requirements in Appendix 1.

## 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.

# **Access to Supplier Personnel and Supplier Information Management System**

## The Buyer may require, and the Supplier must provide the Buyer and its authorised representatives with:

### access to the Supplier Personnel;

### access to the Supplier Information Management System to audit the Supplier and its Subcontractors' compliance with this Agreement; and

### such other information and/or documentation that the Buyer or its authorised representatives may reasonably require,

* 1. to assist the Buyer to establish whether the arrangements which the Supplier and its Subcontractors have implemented in order to ensure the security of the Buyer Data and the Supplier Information Management System are consistent with the representations in the Security Management Plan.

## The Supplier must provide the access required by the Buyer in accordance with paragraph 6.1 within ten Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Buyer with the access that it requires within 24 hours of receipt of such request.

# **Certification Requirements**

## The Supplier shall ensure that, unless otherwise agreed by the Buyer, it is certified as compliant with:

### in the case of a standard consultancy agreement the option chosen by the Buyer in Paragraph 1; or

### in the case of a higher-risk consultancy agreement:

#### 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 27001:2018; and

#### Cyber Essentials Plus (“Relevant Certifications”).

## Unless otherwise agreed by the Buyer, the Supplier must provide the Buyer with a copy of the Relevant Certifications before it begins to provide the Services.

## The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications are:

### currently in effect;

### relate to the full scope of the Supplier Information System; and

### are not subject to any condition that may impact the provision of the Services.

## The Supplier must notify the Buyer promptly, any in any event within three Working Days of becoming aware that:

### a Relevant Certification has been revoked or cancelled by the body that awarded it;

### a Relevant Certification expired and has not been renewed by the Supplier;

### a Relevant Certification no longer applies to the full scope of the Supplier Information Management System or

### 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**”).

## Where the Supplier has notified the Buyer of a Certification Default under paragraph 7.4:

### the Supplier must, within ten working Days of the date in which the Supplier provided notice under paragraph 7.4 (or such other period as the Parties may agree) provide a draft plan (a “**Certification Rectification Plan**”) to the Supplier setting out:

#### full details of the Certification Default, including a root cause analysis;

#### the actual and anticipated effects of the Certification Default;

#### the steps the Supplier will take to remedy the Certification Default;

### the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;

### if the Buyer rejects the Certification Rectification Plan, the Buyer must within five Working Days of the date of the rejection submit a revised Certification Rectification Plan and paragraph 7.5(b) will apply to the re-submitted plan;

### the rejection by the Buyer of a revised Certification Rectification Plan is a material Default of this Agreement;

### if the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

# **Security Management Plan**

## This paragraph 8 applies only where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.

**Preparation of Security Management Plan**

## 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 8 (Security Management) and the Agreement in order to ensure the security of the Buyer Data and the Supplier Information Management System.

## The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Call-Off Contract, the Security Management Plan, which must include:

### an assessment of the Supplier Information Management System against the requirements of this Schedule 8 (Security Management), including Appendix 1

### 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 Buyer Data, the Buyer, the Services and/or users of the Services; and

### the following information in respect of each Sub-contractor:

#### the Sub-contractor’s:

##### legal name;

##### trading name (if any);

##### registration details (where the Sub-contractor is not an individual);

#### the Sites used by the Sub-contractor;

#### the Buyer Data Processed by the Sub-contractor;

#### the Processing that the Sub-contractor will undertake in respect of the Buyer Data;

#### the measures the Sub-contractor has in place to comply with the requirements of this Schedule 8 (Security Management).

## The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and must issue the Supplier with either:

### an information security approval statement, which shall confirm that the Supplier may use the Supplier Information Management System to Process Buyer Data; or

### a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.

## 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 ten Working Days of the date of the rejection, or such other period agreed with the Buyer.

**Updating Security Management Plan**

## 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**

## The Supplier shall notify the Buyer within two Working Days after becoming aware of:

### a significant change to the components or architecture of the Supplier Information Management System;

### a new risk to the components or architecture of the Supplier Information Management System;

### a vulnerability to the components or architecture of the Supplier Information Management System using an industry standard vulnerability scoring mechanism;

* + 1. a change in the threat profile;

### a significant change to any risk component;

### a significant change in the quantity of Personal Data held within the Service;

### a proposal to change any of the Sites from which any part of the Services are provided; and/or

### an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

## Within ten 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.

## 

## Appendix 1: Security Requirements

1. **Location**
   1. Unless otherwise agreed with the Buyer, the Supplier must, and must ensure that its Sub-contractors must, at all times, store, access or process Buyer Data either:
      1. in the United Kingdom;
      2. the European Economic Area; or
      3. in a facility operated by an entity where:
         1. the entity has entered into a binding agreement with the Supplier or Sub-contractor (as applicable);

#### that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Sub-contractors in this Schedule 8 (Security Management);

* + - 1. the Supplier or Sub-contractor has taken reasonable steps to assure itself that
         1. the entity complies with the binding agreement;
         2. any system operated by the Supplier or Sub-contractor has in place appropriate technical and organisational measures to ensure that the Sub-contractor will store, access, manage and/or Process the Government Data as required by this Schedule 8 (*Security Management*); and
      2. the Supplier has provided the Buyer with such information as the Buyer requires concerning:
         1. the entity;
         2. the arrangements with the entity; and
         3. the entity’s compliance with the binding agreement; and
      3. the Buyer has not given the Supplier a Prohibition Notice under paragraph 1.3.
  1. Where the Supplier cannot comply with one or more of the requirements of paragraph 1.1:
     1. it must provide the Buyer with such information as the Buyer requests concerning the security controls in places at the relevant location or locations; and
     2. the Buyer may grant approval to use that location or those locations, and that approval may include conditions; and
     3. if the Buyer does not grant permission to use that location or those locations, the Supplier must cease to store, access or process Buyer Data at that location or those locations within such period as the Buyer may specify.
  2. 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, the storage, access or Processing Buyer Data as specified in the notice (a “**Prohibited Activity ''**).
     1. in any particular country or group of countries;
     2. in or using facilities operated by any particular entity or group of entities; or
     3. 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**”).
  3. Where the Supplier or Sub-contractor, on the date of the Prohibition Notice undertakes any Relevant 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.

1. **Vetting, Training and Staff Access**

**Vetting before performing or managing Services**

* 1. The Supplier must not engage Supplier Personnel, and must ensure that Sub-contractors do not engage Sub-contractor Personnel, in any activity relating to the performance and management of the Services unless:
     1. That individual has passed the security checks listed in paragraph 2.2; or
     2. The Buyer has given prior written permission for a named individual to perform a specific role.
  2. For the purposes of paragraph 2.1, the security checks are:
     1. the checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:
        1. the individual’s identity;
        2. the individual’s nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;
        3. the individual’s previous employment history; and
        4. that the individual has no Relevant Convictions;
     2. national security vetting clearance to the level specified by the Buyer for such individuals or such roles as the Buyer may specify; or
     3. such other checks for the Supplier Personnel of Sub-contractors as the Buyer may specify.

**Annual training**

* 1. 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:
     1. general training concerning security and data handling; and
     2. phishing, including the dangers from ransomware and other malware.

**Staff access**

* 1. 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. 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.
  3. 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**

* 1. Where the Supplier considers it cannot ensure that a Sub-contractors will undertake the relevant security checks on any Sub-contractor Personnel, it must:
     1. as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;
     2. provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Supplier Personnel will perform as the Buyer reasonably requires; and
     3. 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.

1. **Security Testing**
   1. This paragraph applies only where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.
   2. **Note:** the definition of Supplier Information Management System includes those information and communications technology systems that Sub-contractors will use to assist or contribute to the Supplier providing the Services.
   3. The Supplier must, at the Buyer’s option, before providing the Services and when reasonably requested by the Buyer, either:
      1. conduct security testing of the Supplier Information Management System by:
         1. engaging a CHECK Service Provider or a CREST Service Provider;
         2. designing and implementing the testing so as to minimise its impact on the Supplier Information Management System and the delivery of the Services; and
         3. providing the Buyer with a full, unedited and unredacted copy of the testing report without delay and in any event within ten Working Days of its receipt by the Supplier; or
      2. Provide details of any security testing undertaken by a CHECK Service Provider or a CREST Service Provider in respect of the Supplier Information Management System in the calendar year immediately preceding the Buyer’s request or the Effective Date (as appropriate), including:
         1. the parts of the Supplier Information Management System tested;
         2. a full, unedited and unredacted copy of the testing report; and
         3. the remediation plan prepared by the Supplier to address any vulnerabilities disclosed by the security testing; and
         4. the Supplier’s progress in implementing that remediation plan.
   4. The Supplier must remediate any vulnerabilities classified as “medium” or above in the security testing:
      1. before Processing Buyer data where the vulnerability is discovered before the Supplier begins to process Authority Data;
      2. where the vulnerability is discovered when the Supplier has begun to Process Buyer Data:
         1. by the date agreed with the Buyer; or
         2. where no such agreement is reached:
            1. within five Working Days of becoming aware of the vulnerability and its classification where the vulnerability is classified as critical;
            2. within one month of becoming aware of the vulnerability and its classification where the vulnerability is classified as high; and
            3. within three months of becoming aware of the vulnerability and its classification where the vulnerability is classified as medium.
2. **End-user Devices**
   1. The Supplier must manage, and must ensure that all Sub-contractors manage, all End-user Devices on which Buyer Data is stored or processed in accordance the following requirements:
      1. the operating system and any applications that store, process or have access to Buyer Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;
      2. users must authenticate before gaining access;
      3. all Buyer Data must be encrypted using a encryption tool agreed to by the Buyer;
      4. the End-under Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;
      5. 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;
      6. the Supplier or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Buyer Data on the device and prevent any user or group of users from accessing the device;
      7. all End-user Devices are within the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any ISO/IEC 27001:2018 certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.
   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. Where there is any conflict between the requirements of this Schedule 8 (Security Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.
3. **Encryption**
   1. Unless paragraph 5.2 applies, the Supplier must ensure, and must ensure that all Sub-contractors ensure, that Buyer Data is encrypted:
      1. when stored at any time when no operation is being performed on it; and
      2. when transmitted.
   2. Where the Supplier, or a Sub-contractor, cannot encrypt Buyer Data as required by paragraph 5.1, the Supplier must:
      1. 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;
      2. 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;
      3. 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.
   3. 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.
   4. This paragraph applies where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.
   5. Where the Buyer and Supplier reach agreement, the Supplier must update the Security Management Plan to include:
      1. the subset or subsets of Buyer Data not encrypted and the circumstances in which that will occur;
      2. the protective measure that the Supplier and/or Sub-contractor will put in please in respect of the unencrypted Buyer Data.
   6. 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 be determined by an expert in accordance with the Dispute Resolution Procedure.
4. **Access Control**
   1. The Supplier must, and must ensure that all Sub-contractors:
      1. identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;
      2. require multi-factor authentication for all user accounts that have access to Buyer Data or that are Privileged Users;
      3. allow access only to those parts of the Supplier Information Management System and Sites that those persons require;
      4. 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.
   2. 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:
      1. are accessible only from dedicated End-user Devices;
      2. are configured so that those accounts can only be used for system administration tasks;
      3. require passwords with high complexity that are changed regularly;
      4. 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.
   3. The Supplier must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different passwords for their different accounts on the Supplier Information Management System.
   4. The Supplier must, and must ensure that all Sub-contractors:
      1. 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
      2. 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.
5. **Malicious Software**
   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.
   2. The Supplier shall ensure that such Anti-virus Software:
      1. is configured to perform automatic software and definition updates;
      2. performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and
      3. where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.
   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.
   4. Any cost arising out of the actions of the parties taken in compliance with the provisions of paragraph 7.3 shall be borne by the parties as follows:
      1. by the Supplier where the Malicious Software originates from the Supplier Software, any third-party software licenced by the Supplier or the Buyer Data (whilst the Buyer Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and
      2. by the Buyer, in any other circumstance.
6. **Breach of Security**
   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.
   2. The Supplier must, upon becoming aware of a Breach of Security or attempted Breach of Security immediately take those steps identified in the Security Management Plan (if applicable) and all other reasonably steps necessary to:
      1. minimise the extent of actual or potential harm caused by such Breach of Security;
      2. remedy such Breach of Security to the extent possible;
      3. apply a tested mitigation against any such Breach of Security; and
      4. prevent a further Breach of Security in the future which exploits the same root cause failure.
   3. As soon as reasonably practicable and, in any event, within five Working Days, or such other period agreed with the Buyer, following the Breach of Security or attempted Breach of Security, provide to the Buyer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.
   4. The Supplier must take the steps required by paragraph 8.2 at its own cost and expense.
7. **Sub-contractors**
   1. The Supplier must assess the parts of the information and communications technology system and the Sites that its Sub-contractors will use to provide the Services against the NCSC Cloud Security Principles at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-contractor must document that assessment and make that documentation available to the Buyer at the Buyer’s request.
8. **Third-party Software**
   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 Progress the Buyer Data greater than those rights strictly necessary for the use of the software.
9. **Deletion of Buyer Data**
   1. The Supplier must, and must ensure that all Sub-contractors, securely erase any or all Buyer Data held by the Supplier or Sub-contractor when requested to do so by the Buyer using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.