

# 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 13

Schedule 1: Services 35

Schedule 2: Call-Off Contract charges 45

Schedule 3: Collaboration agreement 46

Schedule 4: Alternative clauses 47

Schedule 5: Guarantee 48

Schedule 6: Glossary and interpretations 49

Schedule 7: UK GDPR Information 64

Annex 1: Processing Personal Data 64

Annex 2: Joint Controller Agreement 66

Schedule 8: Security Management 67

# 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** | 754263260887387 |
| **Call-Off Contract reference** | CCIT23B06 |
| **Call-Off Contract title** | The Provision of Resilience Direct Dashboard and Mapping Data Visualisation application |
| **Call-Off Contract description** | The ResilienceDirect™ team are seeking a provider for ResilienceDirect Dashboard and Mapping Data Visualisation application. |
| **Start date** | 15th December 2023 |
| **Expiry date** | 14th December 2025 |
| **Call-Off Contract value** | £1,800,000.00 excluding VAT  £2,160,000.00 including VAT as per PPN 10/21 |
| **Charging method** | Payment will be made on approval of Invoice via BACS |
| **Purchase order number** | Provided post contract award |

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** | REDACTED TEXT under FOIA Section 40, Personal Information |
| **To the Supplier** | REDACTED TEXT under FOIA Section 40, Personal Information |
| **Together the ‘Parties’** | |

### Principal contact details

**For the Buyer:**

REDACTED TEXT under FOIA Section 40, Personal Information

**For the Supplier:**

### REDACTED TEXT under FOIA Section 40, Personal Information

### **Call-Off Contract term**

|  |  |
| --- | --- |
| **Start date** | This Call-Off Contract Starts on **15th December 2023** and is valid for **two (2) years.** |
| **Ending**  **(termination)** | The notice period for the Supplier needed for Ending the Call-Off Contract is at least **90** Working Days from the date of written notice for undisputed sums (as per clause 18.6).  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 12 months, by giving the Supplier **2 weeks** written notice before 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-controls-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 2: Cloud software |
| **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:   * Support & Maintenance * To identify and fix bugs promptly (this is in add onto patching); * Be hosted within the secure ResilienceDirect infrastructure, ensuring best practice for physical and data security. * Provide technical administration and support. * To work closely with RD hosting and infrastructure providers to ensure the mapping capability is backed up, or mirrored, in real-time to a secure Disaster Recovery system. If the live system fails the Disaster Recovery system should immediately be available with the existing information up-to-date. Business as usual on the live system must be restored within a contractually agreed timescale. Any single running operation must be agreed in advance. * For future proofing a mechanism to accommodate an ever growing data file sizes. Best practise would be APIs and Web servers and not zip/shaped files and uploading of excel document that Geo location tagging. * The designed and build should adhere to Government Classification of Official Sensitive including handling. * Daily monitoring checks (for errors and abnormal behaviour). * Patching (critical security patches or regular software releases) * Environment usage checks (e.g. remaining disk space). * Automated database backup monitoring. * Provision of Thunder Forest as a base layer option. * Regular reporting (e.g. number of active users). * Downtime & operational monitoring To maintain site accessibility 24/7/365, with any exceptions or downtime agreed in advance. * An infrastructure move to AWS will require the supplier to work with migration partner. |
| **Location** | The Services will be delivered to ResilienceDirect™ team’s office REDACTED TEXT under FOIA Section 40, Personal Information. However, in light of remote working, the Parties will be collaborating virtually and the services will be delivered remotely. |
| **Quality Standards** | The quality standards required for this Call-Off Contract are:   * ISO 27001:2013 - information security of our business operations and the data that is entrusted to the supplier. * ISO 27017 provides information security controls that must be implemented, specifically relating to cloud services. * ISO 27018:2019 complements much of the data processing responsibilities set out by the GDPR in its aims to protect personal data in addition to EU requirements. * ISO 22301:2012 provides a framework for the continual maintenance and improvement of a business continuity management system. * Cyber Essentials and Cyber Essential Plus government endorsed standard that demonstrates they have the five Cyber Essentials controls implemented. * Adheres to the most current NCSC Security Guidelines - including the 14 Cloud Principles. * NPPV3 Clearance for administration of Servers holding Police data. |
| **Technical Standards:** | The Mapping application is a live service and will need to be supported as such.   * Daily monitoring checks (for errors and abnormal behaviour). * Patching (critical security patches or regular software releases including those highlighted by the Infrastructure and Hosting Provider). * Environment usage checks (e.g. remaining disk space) and to seek approval to increase infrastructure from the ResilienceDirect Team. * Automated database backup monitoring. * Regular reporting (e.g. number of active users.) * 6.3.7 Downtime & operational monitoring. * Bugs/Virus updates, this is addition to the patching. * To identify and fix bugs promptly, ensuring that ResilienceDirect Team are kept informed and agree priority roadmap with them. * Provide technical administration and support. * Engage with our Cabinet Office Security Risk Assessment Advisor and participate in Quarterly ResilienceDirect Security meetings. * Ensure regular liaison with ResilienceDirect hosting and infrastructure provider to mitigate any Disaster Recovery System. If the live system fails the Disaster Recovery system should immediately be available with the existing information up-to-date. Business as usual on the live system must be restored within a contractually agreed timescale. Any single running operation must be agreed in advance. * Be capable of expanding/hosting when required for other services/applications. For example, checking live feeds. * Be expandable to cope with increased community size, additional services like bringing in Application Programmes Interfaces or other live services and products like the Ordinance Survey Data Hub. Whilst always be ready to remedy potential performance issues. * Be able to switch off/sleep when virtual machines are not in use and turn on when required. * The service infrastructure will be a hybrid infrastructure. * All staff involved to have SC clearance. * The successful provider must adhere to National Cyber Security Centre security policies, ideally holding an industry security assurance certification; * The service should be resilient to compromise from basic cyber attacks such as commodity malware ingestion or OWASP vulnerability exploits. * The service must remain accessible from a range of end points including mobile devices; security is paramount regardless of device. * To take action on agreed recommendations from the Cabinet Office Security Risk Assessment Advisor and implement during the contract lifecycle. * At present, the Contracting Authority have in excess of 112,000 users of the Resilience Mapping Application. Although the Volume of Work cannot be guaranteed. |
| **Service level agreement:** |  |
| **Onboarding** | Airbox provides remote or on-site train-the-trainer training dependent on client requirements, to be agreed in advance.  User manuals and e-learning will be sent to client upon activation of software. |

|  |  |
| --- | --- |
| **Offboarding** | The client contacts identified on the ISO 27001 and GDPR compliant Client Data Management form will be contacted by Airbox to confirm whether data should be extracted or deleted.  On the day of contract termination, access to the server through the clients devices will be removed.  Client contacts will be contacted by their Key Account Manager or Account Manager to confirm whether data should be extracted or deleted. |
| **Limit on Parties’ liability** | The annual total liability of either Party for all Property defaults will not exceed £1,000,000.00 (One Million Pounds GBP). The annual total liability for Buyer Data defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the CallOff Contract Term (whichever is the greater). The annual total liability for all other defaults will not exceed the greater of in year 1 £600,000.0 (Six Hundred Thousand Pounds) and Year 2 £600,000.00 (Six Hundred Thousand Pounds) or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). The insurance(s) required will be:  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 |
| **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** | The Buyer is responsible for **N/A**. |
| **Buyer’s equipment** | The Buyer’s equipment to be used with this Call-Off Contract includes **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** | The payment profile for this Call-Off Contract is monthly in arrears |
| **Invoice details** | The Supplier will issue electronic invoices monthly in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice. |
| **Who and where to send invoices to** | REDACTED TEXT under FOIA Section 40, Personal Information |
| **Invoice information required** | All invoices must include:  ● The Purchase Order number  ● Contract reference  ● Date  ● Address (Buyer and Supplier)  ● Supplier name and contact details  ● Remittance and payment bank account details  ● Description of the charges  ● Volume of the charges  ● Unit cost of the charges |
| **Invoice frequency** | Invoice will be sent to the Buyer monthly |
| **Call-Off Contract value** | The total value of this Call-Off Contract is £1,800,000.00 ( 2+1) excluding VAT  £2,160,000.00 including VAT as per PPN 10/21 |
| **Call-Off Contract charges** | REDACTED TEXT under FOIA Section 43 Commercial Interests |

### Additional Buyer terms

|  |  |
| --- | --- |
| **Performance of the** **Service** | This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones: |
| **Guarantee** | N/A |
| **Supplemental requirements in addition to the Call-Off** **terms** | Within the scope of the Call-Off Contract, the Supplier will: Due to the nature of the work there may be national crises/major incidents that require development or enhancements and flexibility or revising priorities. Achieving elastic scaling will require application and infrastructure changes, so both the supplier and existing hosting and infrastructure provider will need to collaborate. For example, we could have a surge in users. |
| **Alternative clauses** | N/A |
| **Buyer specific**  **amendments**  **to/refinements of the Call-Off Contract terms** | Security Schedule 8 (Security Management) is used |
| **Personal Data and** **Data Subjects** | Annex 1 of Schedule 7 is being used |
| **Intellectual Property** | N/A |
| **Social Value** | The expectation is for the supplier to make a positive impact through its activities on the Resilience community as per the Social Value section of GCloud 13 Service: 754263260887387:  Fighting climate change:  Yes, a copy of Social Action Plan can be provided upon request.  Covid-19 recovery:  Yes, a copy of Social Action Plan can be provided upon request.  Tackling economic inequality:  Yes, a copy of Social Action Plan can be provided upon request.  Equal opportunity:  Yes, a copy of Social Action Plan can be provided upon request.  Wellbeing:  Yes, a copy of Social Action Plan can be provided upon request. |

### 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** |  |  |
| **Date** | [**Enter date**] | [**Enter date**] |

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 14digit 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 invoices 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 trade marks 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 judgment 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

1. 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 Call-Off Contract by giving 30 days notice to the Supplier.

### 33. Data Protection Legislation (GDPR)

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

reproduced in this Call-Off Contract document at Schedule 7.

# 

# **Schedule 1: Services**

# **PURPOSE**

1.1 The ResilienceDirect™ Team (RD), a section within the Resilient Directorate that is part of the Economic and Domestic Secretariat within the Cabinet Office, are seeking a provider for the delivery of the ResilienceDirect Dashboard and Mapping application

1.2 Due to the nature of the requirement, addressing the threats and hazards to the UK including ‘black swan’ events (i.e. an event or occurrence that deviates beyond what is normally expected of a situation and is therefore extremely difficult to predict, potentially having a major effect), security relating to the support of the Resilient Directorate and Ministers is a key delivery.

1.3 ResilienceDirect™ (RD) is the UK’s free-to-use, 24/7/365 secure web based service for all Category 1 & 2 responders, government departments and other key organisations in the UK resilience community to securely share information during emergency responses, planning exercises and recovery. The service has in excess of 105,000 registered user accounts and comprises a number of applications including:

1.4 Collaborate is a secure information sharing application where users can upload documents, create pages and share information securely with other users across the community or within closed groups.

1.5 Mapping is a secure data visualisation application where users are able to create, edit and share maps with a set of functional tools.  The mapping application enables users to upload and visualise multiple datasets as well as providing access to a variety of centralised live data feeds such as Meteorological Office’s Rainfall and Environment Agency’s Flooding data.

1.6 Our Learning and development area  (JOL online) is run by the Training and Exercising Team, in the Resilience Directorate. This Team leads on sharing and encourages best practice across the resilience community in order to inform exercising, planning and response.

2.1.4 The Dashboard is the ResilienceDirect landing page that provides links to the various ResilienceDirect applications and interfaces with Twitter to display the ResilienceDirect Twitter feed.

2.1.5 The various ResilienceDirect applications are provided by 3rd party suppliers with whom the hosting provider will need to work closely.

# **BACKGROUND TO THE BUYER**

## The Cabinet Office supports the Prime Minister and ensures the effective running of government. The Cabinet Office is also the corporate headquarters for government, in partnership with HM Treasury, and takes the lead in certain critical policy areas. The Resilience Directorate is a part of the Economic and Domestic Secretariat which itself is a department of the Cabinet Office that is responsible for driving forward the UK Government’s work on national resilience, managing the resilience system, resilience frameworks and risk processes.

# **Background to requirement/OVERVIEW of requirement**

## The service is to be procured under the Crown Commercial Service Framework G-Cloud 13 with requirements that fall into the three lots of Cloud Hosting, Cloud Software and Cloud Support.

## The general requirements are provided in section 5, with the Cloud Hosting, Software and Cloud Support specific requirements covered in sections 6, 7 and 8.

# **definitions**

|  |  |
| --- | --- |
| Abbreviation | Meaning |
| AV | Anti-Virus (including Anti-Malware) |
| BC | Business Continuity |
| BCP | Business Continuity Plan |
| DEV | Development |
| DKIM | Domain Keys Identified Mail |
| DMARC | Domain-based Message Authentication, Reporting and Conformance |
| DR | Disaster Recovery |
| EA | Environment Agency |
| EP | Emergency Planning |
| EWS | Early Warning System (provided by NCSC) |
| GDPR | General Data Protection Regulations |
| GPG | Good Practice Guide |
| HM | Her Majesty |
| HMG | Her Majesty's Government |
| ITSHC | Information Technology Security Health Check |
| JOL | Joint Organisational Learning |
| MS | Microsoft |
| NCSC | National Cyber Security Centre |
| NRA | National Risk Assessment |
| OVF | Open Virtualisation Format |
| PROD | Production |
| RD | ResilienceDirect™ |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| SAN | Storage Area Network |
| SC | Security Check |
| SLA | Service Level Agreement |
| SPF | Sender Policy Framework |
| SQL | Structured Query Language (MS SQL application software in the context of RD) |
| SSH | Secure Socket Shell |
| SSL | Secure Sockets Layer |
| SSO | Single Sign On |
| TB | Terabyte |
| UAT | User Acceptance Test |
| UK | United Kingdom |
| URL | Uniform Resource Locator |
| VM | Virtual Machine |
| WSUS | Windows Update Service |

# **scope of requirement**

### To ensure maintenance of the live ResilienceDirect mapping capability is provided and this to include regular security patching, fixing on bugs and enhancements to retire any part of code or technology that is no longer industry standard or a security vulnerability/cyber threat has been identified.

# **The requirement**

### Support & Maintenance

### To identify and fix bugs promptly (this is in add onto patching);

### Be hosted within the secure ResilienceDirect infrastructure, ensuring best practice for physical and data security.

### Provide technical administration and support.

### To work closely with RD hosting and infrastructure providers to ensure the mapping capability is backed up, or mirrored, in real-time to a secure Disaster Recovery system. If the live system fails the Disaster Recovery system should immediately be available with the existing information up-to-date. Business as usual on the live system must be restored within a contractually agreed timescale. Any single running operation must be agreed in advance.

### For future proofing a mechanism to accommodate an ever growing data file sizes. Best practise would be APIs and Web servers and not zip/shaped files and uploading of excel document that Geo location tagging.

### The designed and build should adhere to Government Classification of Official Sensitive including handling.

### Daily monitoring checks (for errors and abnormal behaviour).

### Patching (critical security patches or regular software releases)

### Environment usage checks (e.g. remaining disk space).

### Automated database backup monitoring.

### Regular reporting (e.g. number of active users).

### Downtime & operational monitoring To maintain site accessibility 24/7/365, with any exceptions or downtime agreed in advance.

### An infrastructure move to AWS will require the supplier to work with migration partner.

## **Development**

### Support and Maintenance is continuous and development is as directed by the Cabinet Office ResilienceDirect Team as technology is forever evolving and we many need to develop additional mapping capability.

### To work in conjunction with other ResilienceDirect suppliers to ensure Single Sign On works seamlessly with the ResilienceDirect mapping capability. This is to also include the single sign on the dashboard.

### To ensure mapping capabilities are agile and meet the ResilienceDirect community users needs.

### Provison of thunder forest

### To ensure system interoperability with other core ResilienceDirect capabilities for example to develop the product to allow documents and plans to be displayed within a map.

## **System Monitoring of RD Mapping.**

### The Mapping application is a live service and will need to be supported as such.

### Daily monitoring checks (for errors and abnormal behaviour).

### Patching (critical security patches or regular software releases including those highlighted by the Infrastructure and Hosting Provider).

### Environment usage checks (e.g. remaining disk space) and to seek approval to increase infrastructure from the ResilienceDirect Team.

### Automated database backup monitoring.

### Regular reporting (e.g. number of active users.)

### Downtime & operational monitoring.

### Bugs/Virus updates, this is addition to the patching.

### To identify and fix bugs promptly, ensuring that ResilienceDirect Team are kept informed and agree priority roadmap with them.

### Provide technical administration and support.

### Engage with our Cabinet Office Security Risk Assessment Advisor and participate in Quarterly ResilienceDirect Security meetings.

### Ensure regular liaison with ResilienceDirect hosting and infrastructure provider to mitigate any Disaster Recovery System. If the live system fails the Disaster Recovery system should immediately be available with the existing information up-to-date. Business as usual on the live system must be restored within a contractually agreed timescale. Any single running operation must be agreed in advance.

### Be capable of expanding/hosting when required for other services/applications. For example, checking live feeds.

### Be expandable to cope with increased community size, additional services like bringing in Application Programmes Interfaces or other live services and products like the Ordinance Survey Data Hub. Whilst always be ready to remedy potential performance issues.

### Be able to switch off/sleep when virtual machines are not in use and turn on when required.

### The service infrastructure will be a hybrid infrastructure.

### All staff involved to have SC clearance.

### The successful provider must adhere to National Cyber Security Centre security policies, ideally holding an industry security assurance certification;

### The service should be resilient to compromise from basic cyber attacks such as commodity malware ingestion or OWASP vulnerability exploits.

### The service must remain accessible from a range of end points including mobile devices; security is paramount regardless of device.

### To take action on agreed recommendations from the Cabinet Office Security Risk Assessment Advisor and implement during the contract lifecycle.

### At present, the Contracting Authority have in excess of 112,000 users of the Resilience Mapping Application. Although the Volume of Work cannot be guaranteed.

# **key milestones and Deliverables**

## The following Contract milestones/deliverables shall apply:

|  |  |  |
| --- | --- | --- |
| Milestone/Deliverable | Description | Timeframe or Delivery Date |
| 1 | Provide technical administration and support as per our priorities.  See table 2 | Within week 1 of the Contract Award |
| 2 | Resolution time for bug fixes  Depending on the severity of the bug. For example, if it interrupted the service, the expectation of resolution would be from 1 day up to 1 week. Bugs which had a low impact on the service, expectation of resolution would be one month. | See table 2 |

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Service Level Target | Minimum Service Level | Service Credits |
| P1  Incidents | 100% of Incidents responded to within 30 minutes – 24x7 Service Hours | 100 % | 1st incident missed response time – 5% Service Credit 2nd incident missed response time – 10% Service Credit |
| P2  Incidents | 100% of Incidents responded to within 1 Normal Business Hour. | Service credits apply from 2nd failure within a calendar Month | 1st incident missed response time – 0% Service Credit 2nd incident missed response time – 5% Service Credit 3rd incident missed response time – 10% Service Credit |
| P3  Incidents | 100% of Incidents responded to within 4 Normal Business Hours | None | No Service Credit |
| P4  Incidents | 100% of Incidents responded to within 1 Working day | None | No Service Credit |
| Root Cause | 100% of P1 Incidents to receive a Root Cause Analysis within 10 Working Days of Resolution | None | No Service Credit |
| Availability of core  Application | 100% | 99.75% | Availability 99.75% to 99.51% – 2% Service Credit per month. 99.50% or 99.26% - 5% Service Credit per month 99.25% or less – 10% Service Credit per month |

# **MANAGEMENT INFORMATION/reporting**

## Management information at our regular fortnightly meetings, annual service review and engage in the quarterly Security review.

# **volumes**

## ResilienceDirect registered users have increased from 30,000 in 2018 to over 83,000 in March 2021 to currently over 112,000 in October 2023.  The purpose of ResilienceDirect is to support emergency planning, exercise response and recovery for the whole  UK and it overseas territories there is no limit on the number of users  to support HMGs mission to save lives and aim to keep the UK safe.  This supports the National Risk Assumptions and the National Security Risk Assessment.

## This is a Call Off Contract so volumes of work cannot be guaranteed you might have a lower demand or no demand at all.   However, this live service will always need support and maintenance as a minimum

# **continuous improvement**

## The supplier will be expected to continually improve the way in which the required services are to be delivered throughout the contract duration.

## The Supplier should present new ways of working to the ResilienceDirect Team during weekly Contract service review meetings.

## Changes to the way in which the Service is to be delivered must be brought to the Authority’s attention and agreed prior to any changes being implemented.

## All proposed changes must comply with gov.uk service standards. The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

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

## Changes to the way in which the Services are to be delivered must be brought to the Buyer’s attention and agreed prior to any changes being implemented

# **Sustainability / SOCIAL VALUE**

## The supplier must take steps to minimise it’s carbon footprint by operating procedures being as innovative as possible and taking into account environmental impacts.

## The suppliers should ensure all staff are aware of social values and fully trained in inclusion and diversity laws and policies.

# **quality**

## The quality standards required for this Call-Off Contract are:

## ISO 27001:2013 - information security of our business operations and the data that is entrusted to the supplier.

## ISO 27017 provides information security controls that must be implemented, specifically relating to cloud services.

## ISO 27018:2019 complements much of the data processing responsibilities set out by the GDPR in its aims to protect personal data in addition to EU requirements.

## ISO 22301:2012 provides a framework for the continual maintenance and improvement of a business continuity management system.

## Cyber Essentials and Cyber Essential Plus government endorsed standard that demonstrates they have the five Cyber Essentials controls implemented.

## Adheres to the most current NCSC Security Guidelines - including the 14 Cloud Principles.

## NPPV3 Clearance for administration of Servers holding Police data.

# **PRICE**

## The contract is capped to a maximum of (at a maximum of £600,000 per annum for 2+1).

## Prices are to be submitted to Resilience direct , via email   [resiliencedirect@cabinetoffice.gov.uk](mailto:resiliencedirect@cabinetoffice.gov.uk) and including VAT and all other expenses relating to Contract delivery clearly highlighted.

# **STAFF AND CUSTOMER SERVICE**

## The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.

## The Supplier’s staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

## The Supplier shall ensure that staff understand the Buyer’s vision and objectives and will provide excellent customer service to the Buyer throughout the duration of the Contract.

# **service levels and performance**

## The Buyer will measure the quality of the Supplier’s delivery by:

|  |  |  |  |
| --- | --- | --- | --- |
| KPI/SLA | Service Area | KPI/SLA description | Target |
| 1 | Service  Availability | If the service becomes unavailable, have the hosting/infrastructure back up ASAP or within an hour, and an incident report with the RD team within 24 hours. | 99.75% |
| 2 | Resolution time for bug fixes | Depending on the severity of the bug.  For example, if it interrupted the service, the expectation of resolution would be from 1 day up to 1 week.  Bugs which had a low impact on the service, expectation of resolution would be one month. | 99.7% |
| 3 | Quality of development and delivery of project plans | Continuously review the service level Agreements that are part of the contract and the key performance Indicators against the Service Offerings to ensure that all requested work is delivered. | 99% |
| 4 | Query response time | Within 24 hours. Whether it be from the RD support desk or RD team, excluding weekends. If it is a priority 1 then the out of hours triage is activated and we expect a response within the hour. | 99.7% |
| 5 | Team sustainability | The supplier shall ensure that their delivery teams are adequately resourced and with the required capability to support and sustain the RD service, thereby not falling prey to any single point of failure. | 99.9% |
| 6 | Notification of planned maintenance work | The supplier shall advise the Authority and their suppliers of any planned maintenance activities at least 1 week in advance | 99.7% |

## Where a Supplier fails the KPIs above, the Authority will, in the first instance, seek a mutually agreeable resolution with the Supplier. However, if this is not possible, the Authority reserves the right to cancel the agreement and seek alternative supply.

## You have a no fault termination clause. We can cancel the contract at any time giving 30 day notice. We would expect the supplier to hand over any detailed instructions of how the service operates.

# **Security and CONFIDENTIALITY requirements**

## All staff involved have SC clearance.

## The successful provider must adhere to National Cyber Security Centre security policies, ideally holding an industry security assurance certification;

## The service should be resilient to compromise from basic cyber attacks such as commodity malware ingestion or OWASP vulnerability exploits;

## To implement the agreed recommendations from the ResilienceDirect risk assessment throughout contract lifecycle.

## Adhere to the security schedule in Annex A.

# **payment AND INVOICING**

## Invoicing to be made calendar monthly in arrears.

## Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

## Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

## Invoices should be submitted to: REDACTED TEXT under FOIA Section 40, Personal Information.

## The service provider must be UK based. This is in order to protect the integrity of the platform and to ensure that the information hosted on it is kept as secure as possible;

## The location of the Services will be carried out virtually and in both the supplier’s premises and REDACTED TEXT under FOIA Section 40, Personal Information.

## **CONTRACT MANAGEMENT**

## Attendance at Contract Review meetings shall be at the Supplier’s own expense.

## The supplier will provide progress updates and clear actions as agreed during these meetings.

## The contract will commence on 15 December 2023 for 24 months, ending on 14 December 2025; this will take the form of a 1+1 Year contract, i.e. the contract will span for 1 year, be evaluated and continue for a further year provided both supplier and customer are satisfied. A review will take place at this time to ascertain the continued quality of the service. As a G-Cloud call-off contract, the contract can be terminated with at least 30 days’ written notice for “Ending without cause”.

## 

# **Location**

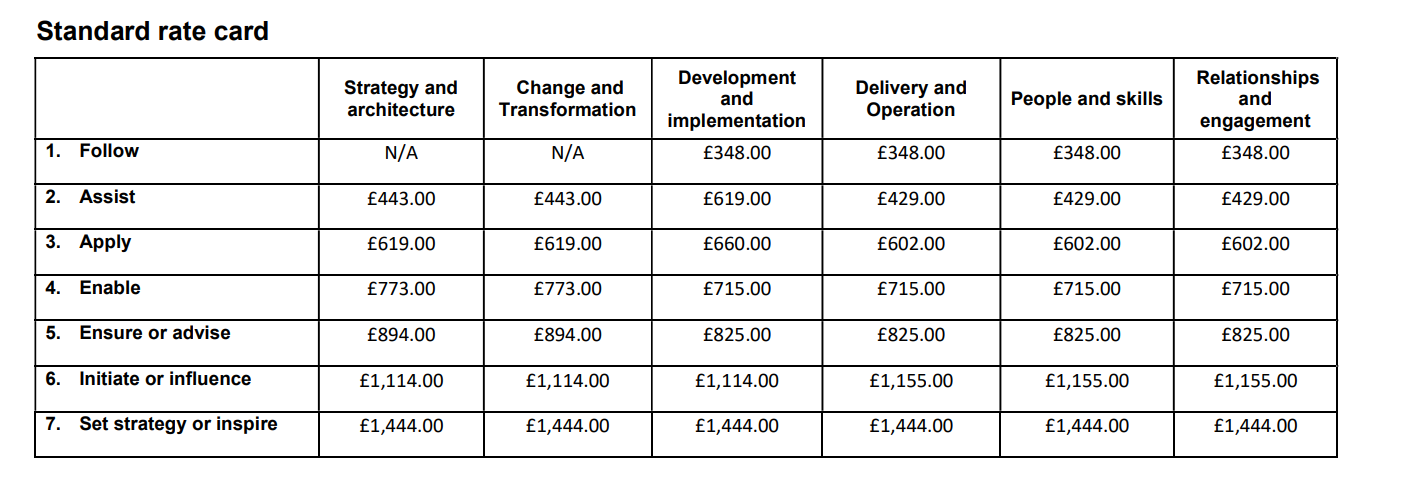
The location of the Services will be carried out at REDACTED TEXT under FOIA Section 40, Personal Information.

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

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

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:

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



# **Schedule 3: Collaboration agreement (Not used)**

## Schedule 4: Alternative clauses (Not used)

### 

## Schedule 5: Guarantee (Not used)

## Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

|  |  |
| --- | --- |
| **Expression** | **Meaning** |
| **Additional Services** | Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request. |
| **Admission Agreement** | The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s). |
| **Application** | The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform). |
| **Audit** | An audit carried out under the incorporated Framework Agreement clauses. |
| **Background IPRs** | 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-todate 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 * 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, judgment 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, judgment, 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:   + under the Bribery Act 2010   + under legislation creating offences concerning Fraud   + at common Law concerning Fraud   + committing or attempting or conspiring to commit Fraud |

|  |  |
| --- | --- |
| **Project Specific IPRs** | Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier’s Background IPRs. |
| **Property** | Assets and property including technical infrastructure, IPRs and equipment. |
| **Protective Measures** | Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it. |
| **PSN or Public Services** **Network** | The Public Services Network (PSN) is the government’s high performance network which helps public sector organisations work together, reduce duplication and share resources. |
| **Regulatory body or bodies** | Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract. |
| **Relevant person** | Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body. |
| **Relevant Transfer** | A transfer of employment to which the employment regulations applies. |
| **Replacement Services** | Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-  Off Contract, whether those services are provided by the Buyer or a third party. |
| **Replacement supplier** | Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer). |
| **Security management plan** | The Supplier's security management plan developed by the Supplier in accordance with clause 16.1. |

|  |  |
| --- | --- |
| **Services** | The services ordered by the Buyer as set out in the Order Form. |
| **Service data** | Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data. |
| **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 G-Cloud Services or any part thereof. |
| **Subcontractor** | Any third party engaged by the Supplier under a subcontract  (permitted under the Framework Agreement and the Call-Off  Contract) and its servants or agents in connection with the provision of G-Cloud Services. |
| **Subprocessor** | Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract. |
| **Supplier** | The person, firm or company identified in the Order Form. |
| **Supplier Representative** | The representative appointed by the Supplier from time to time in relation to the Call-Off Contract. |

|  |  |
| --- | --- |
| **Supplier staff** | All persons employed by the Supplier together with the Supplier’s servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract. |
| **Supplier Terms** | The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier’s Application. |
| **Term** | The term of this Call-Off Contract as set out in the Order Form. |
| **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.

1.1 The contact details of the Buyer’s Data Protection Officer are : dpo@cabinetoffice.gov.uk

1.2 The contact details of the Supplier’s Data Protection Officer are: compliance@airboxsystems.com

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

|  |  |
| --- | --- |
|  |  |
| **Description** | **Details** |
| Identity of Controller for each Category of Personal Data | **The Buyer is Controller and the Supplier is Processor**  The Buyer is Controller and the Supplier is Processor The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, Buyer is the Controller and the Supplier is the Processor of the Personal Data recorded below |

|  |  |
| --- | --- |
| Duration of the Processing | Up to 7 years after the expiry or termination of the Framework Agreement |
| Nature and purposes of the Processing | Personal data is stored on ResilienceDirect to allow multi- organisation users to log into the Service. Users may also choose to store data relating to the general public such as location in the event of a response to an incident/emergency. |
| Type of Personal Data | User IDs (unique to the user)  Names (compulsory)  Email addresses (compulsory)  Personal emails (optional)  Telephone numbers –  (optional)  Any information that is recorded by emergency responders such as location. |

|  |  |
| --- | --- |
| Categories of Data Subject | Employees of multiple organisations involved in contingency activities, eg first responders and members of the public who become involved in emergency situations. |
| 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 | As outline in the security Schedule 8 para 12 and 19 e.g. encryption when at rest or in transit and deleted at our request |

## 

## Annex 2: Joint Controller Agreement (Not used)

Schedule 8 - Security Management

# **1 Supplier obligations**

**Core requirements**

## The Supplier must comply with the core requirements set out in Paragraphs 3 to 8.

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

|  |  |  |
| --- | --- | --- |
| Certifications (see Paragraph 3) | | |
| The Supplier must have the following Certifications: | ISO/IEC 27001:2013 by a UKAS-approved certification body | ☒ |
| Cyber Essentials Plus | ☒ |
| Cyber Essentials | ☒ |
| Subcontractors that Process Government Data must have the following Certifications: | ISO/IEC 27001:2013 by a UKAS-approved certification body | ☒ |
| Cyber Essentials Plus | ☒ |
| Cyber Essentials | ☒ |
| Locations (see Paragraph 4) | | |
| The Supplier and Subcontractors may store, access or Process Government Data in: | the United Kingdom only | ☒ |
| the United Kingdom and European Economic Area only | ☐ |
| anywhere in the world not prohibited by the Buyer | ☐ |

**Optional requirements**

## Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements of the corresponding paragraph. Where the Buyer has not selected an option, the corresponding requirement does not apply.

|  |  |
| --- | --- |
| Security testing (see Paragraph 9) | |
| The Supplier must undertake security testing at least once every Contract Year and remediate any vulnerabilities, where it is technically feasible to do so | ☒ |
| Cloud Security Principles (see Paragraph 10) | ☒ |
| The Supplier must assess the Supplier System against the Cloud Security Principles | ☒ |
| Record keeping (see paragraph 11)☒ | |
| The Supplier must keep records relating to Subcontractors, Sites, Third Party Tools and third parties | ☒ |
| Encryption (see Paragraph 12) | |
| The Supplier must encrypt Government Data while at rest or in transit |  |
| Protecting Monitoring System (see Paragraph 13) |  |
| The Supplier must implement an effective Protective Monitoring System | ☒ |
| Patching (see Paragraph 14) |  |
| The Supplier must patch vulnerabilities in the Supplier System promptly | ☒ |
| Malware protection (see Paragraph 15) |  |
| The Supplier must use appropriate Anti-virus Software | ☒ |
| End-user Devices (see Paragraph 16) |  |
| The Supplier must manage End-user Devices appropriately |  |
| Vulnerability scanning (see Paragraph 17) | |
| The Supplier must scan the Supplier System monthly for unpatched vulnerabilities | ☒ |
| Access control (see paragraph 18) |  |
| The Supplier must implement effective access control measures for those accessing Government Data and for Privileged Users | ☒ |
| Return and deletion of Government Data (see Paragraph 19) | |
| The Supplier must return or delete Government Data when requested by the Buyer |  |
| Physical security (see Paragraph 20) | |
| The Supplier must store Government Data in physically secure locations | ☒ |
| Security breaches (see Paragraph 21) | |
| The Supplier must report any Breach of Security to the Buyer promptly | ☒ |
| Security Management Plan (see Paragraph 22) |  |
| The Supplier must provide the Buyer with a Security Management Plan detailing how the requirements for the options selected have been met. | ☒ |

# **Definitions**

|  |  |
| --- | --- |
| “Anti-virus Software” | means software that:   * + 1. protects the Supplier System from the possible introduction of Malicious Software;     2. scans for and identifies possible Malicious Software in the Supplier System;     3. if Malicious Software is detected in the Supplier System, so far as possible:        1. prevents the harmful effects of the Malicious Software; and        2. removes the Malicious Software from the Supplier System; |
| “Contract Year” | means:   * + 1. a period of 12 months commencing on the Effective Date;     2. thereafter a period of 12 months commencing on each anniversary of the Effective Date;     3. with the final Contract Year ending on the expiry or termination of the Term; |
| “CREST Service Provider” | means a company with an information security accreditation of a security operations centre qualification from CREST International; |
| “Government Data” | 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;     2. Personal Data for which the Buyer is a, or the, Data Controller; or     3. any meta-data relating to categories of data referred to in paragraphs (a) or (b);   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; and   for the avoidance of doubt includes the Code and any meta-data relating to the Code. |
| “Certifications” | means one or more of the following certifications:   * + 1. ISO/IEC 27001:2013 by a UKAS-approved certification body in respect of the Supplier System, or in respect of a wider system of which the Supplier System forms part; and     2. Cyber Essentials Plus; and/or     3. Cyber Essentials; |
| “Breach of Security” | means the occurrence of:   * + 1. any unauthorised access to or use of the Services, the Sites, the Supplier System and/or the Government Data;     2. the loss (physical or otherwise), corruption and/or unauthorised disclosure of any Government Data, including copies of such Government Data; and/or     3. any part of the Supplier System ceasing to be compliant with the required Certifications;     4. the installation of Malicious Software in the Supplier System:     5. any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the Supplier System; and     6. includes any attempt to undertake the activities listed in sub-paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:        1. was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or        2. was undertaken, or directed by, a state other than the United Kingdom; |
| “CHECK Scheme” | means the NCSC’s scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks; |
| “CHECK Service Provider” | means a company which, under the CHECK Scheme:   * + 1. has been certified by the NCSC;     2. holds “Green Light” status; and     3. is authorised to provide the IT Health Check services required by Paragraph 5.2 (*Security Testing*); |
| “Cloud Security Principles” | means the NCSC’s document “Implementing the Cloud Security Principles” as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/ implementing-the-cloud-security-principles. |
| “Cyber Essentials” | means the Cyber Essentials certificate issued under the Cyber Essentials Scheme; |
| “Cyber Essentials Plus” | means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme; |
| “Cyber Essentials Scheme” | means the Cyber Essentials scheme operated by the NCSC; |
| “End-user Device” | means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic devices used in the provision of the Services; |
| “IT Health Check” | means testing of the Supplier Information Management System by a CHECK Service Provider; |
| “Malicious Software” | means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations; |
| “NCSC” | means the National Cyber Security Centre, or any successor body performing the functions of the National Cyber Security Centre; |
| “NCSC Device Guidance” | means the NCSC’s document “Device Security Guidance”, as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance; |
| “Privileged User” | means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges; |
| “Process” | means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data; |
| “Prohibition Notice” | means the meaning given to that term by Paragraph 4.4. |
| “Protective Monitoring System” | has the meaning given to that term by Paragraph 13.1; |
| “Relevant Conviction” | 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; |
| “Sites” | means any premises (including the Buyer’s Premises, the Supplier’s premises or third party premises):   * + 1. from, to 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 System is situated; or        2. any physical interface with the Authority System takes place; |
| “Standard Contractual Clauses” | means, for the purposes of this Schedule 8 (*Security Management*):   * + 1. the standard data protection paragraphs specified in Article 46 of the UK GDPR setting out the appropriate safeguards for the transmission of personal data outside the combined territories of the United Kingdom and the European Economic Area;     2. as modified to apply equally to the Government Data as if the Government Data were Personal Data; |
| “Subcontractor Personnel” | 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; or        2. the provision of facilities or services that are necessary for the provision of the Services; |
| "Supplier System” | means   * + 1. any:        1. information assets,        2. IT systems,        3. IT services; or        4. Sites,   that the Supplier or any Subcontractor will use to Process, or support the Processing of, Government Data and provide, or support the provision of, the Services; and   * + 1. the associated information management system, including all relevant:        1. organisational structure diagrams;        2. controls;        3. policies;        4. practices;        5. procedures;        6. processes; and        7. resources; |
| “Third-party Tool” | means any activity conducted other than by the Supplier during which the Government Data is accessed, analysed or modified, or some form of operation is performed on it; |

# **Part One: Core Requirements**

# **Certification Requirements**

## Where the Buyer has not specified Certifications under Paragraph 1, the Supplier must ensure that it and any Subcontractors that Process Government Data are certified as compliant with Cyber Essentials.

## Where the Buyer has specified Certifications under Paragraph 1, the Supplier must ensure that both:

### it; and

### any Subcontractor that Processes Government Data,

## are certified as compliant with the Certifications specified by the Buyer in Paragraph 1:

## The Supplier must ensure that the specified Certifications are in place for it and any relevant Subcontractor:

### before the Supplier or any Subcontractor Processes Government Data; and

### throughout the Term.

# **Location**

## Where the Buyer has not specified any locations or territories in Paragraph 1, the Supplier must not, and ensure that Subcontractors do not store, access or Process Government Data outside the United Kingdom.

## Where the Buyer has specified locations or territories in Paragraph 1, the Supplier must, and ensure that its Subcontractors, at all times store, access or process Government Data only in or from the geographic areas specified by the Buyer.

## Where the Buyer has permitted the Supplier and its Subcontractors to store, access or process Government Data outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Subcontractors store, access or process Government Data in a facility operated by an entity where:

### the entity has entered into a binding agreement with the Supplier or Subcontractor (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 5 (*Security Management*);

### the Supplier or Subcontractor has taken reasonable steps to assure itself that:

#### the entity complies with the binding agreement; and

#### the Subcontractor’s system 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*);

### the Buyer has not given the Supplier a Prohibition Notice under Paragraph 4.4.

## The Buyer may by notice in writing at any time give notice to the Supplier that it and its Subcontractors must not undertake or permit to be undertaken the storage, accessing or Processing of Government Data in one or more countries or territories (a “**Prohibition Notice**”).

## Where the Supplier must and must ensure Subcontractors comply with the requirements of a Prohibition Notice within 40 Working Days of the date of the notice.

# **Staff vetting**

## The Supplier must not allow Supplier Personnel, and must ensure that Subcontractors do not allow Subcontractor Personnel, to access or Process Government Data, if that person:

### has not completed the Staff Vetting Procedure; or

### where no Staff Vetting Procedure is specified in the Order Form:

#### has not undergone the checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:

##### the individual’s identity;

##### where that individual will work in the United Kingdom, the individual’s nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom; and

##### the individual’s previous employment history; and

##### that the individual has no Relevant Convictions; and

#### has not undergone national security vetting clearance to the level specified by the Authority for such individuals or such roles as the Authority may specify

# **Supplier assurance letter**

## The Supplier must, no later than the last day of each Contract Year, provide to the Buyer a letter from its Chief Technology Officer (or equivalent officer) confirming that, having made due and careful enquiry:

### the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters required by this Agreement;

### it has fully complied with all requirements of this Schedule 8 (Security Management); and

### all Subcontractors have complied with the requirements of this Schedule 8 (Security Management) with which the Supplier is required to ensure they comply;

### the Supplier considers that its security and risk mitigation procedures remain effective.

# **Assurance**

## The Supplier must provide such information and documents as the Buyer may request in order to demonstrate the Supplier’s and any Subcontractors’ compliance with this Schedule 8 (*Security Management*).

## The Supplier must provide that information and those documents:

### within 10 Working Days of a request by the Buyer;

### except in the case of original document, in the format and with the content and information required by the Buyer; and

### in the case of original document, as a full, unedited and unredacted copy.

# **Use of Subcontractors and third parties**

## The Supplier must ensure that Subcontractors and any other third parties that store, have access to or Process Government Data comply with the requirements of this Schedule 8(Security Management).

# **Part Two: Additional Requirements**

# **Security testing**

## The Supplier must:

### before Processing Government Data;

### at least once during each Contract Year; and

## undertake the following activities:

### conduct security testing of the Supplier System (an “**IT Health Check**”) in accordance with Paragraph 9.2; and

### implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph 9.3.

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

### use only a CHECK Service Provider or CREST Service Provider to perform the IT Health Check;

### design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier System and the delivery of the Services;

### ensure that the scope of the IT Health Check encompasses the components of the Supplier System used to access, store, Process or manage Government Data; and

### ensure that the IT Health Check provides for effective penetration testing of the Supplier System.

## The Supplier treat any vulnerabilities as follows:

### the Supplier must remedy any vulnerabilities classified as critical in the IT Health Check report:

#### if it is technically feasible to do so, within 5 Working Days of becoming aware of the vulnerability and its classification; or

#### if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 9.3(a)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

### the Supplier must remedy any vulnerabilities classified as high in the IT Health Check report:

#### if it is technically feasible to do so, within 1 month of becoming aware of the vulnerability and its classification; or

#### if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 9.3(b)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

### the Supplier must remedy any vulnerabilities classified as medium in the IT Heath Check report:

#### if it is technically feasible to do so, within 3 months of becoming aware of the vulnerability and its classification; or

#### if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 9.3(c)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

### where it is not technically feasible to remedy the vulnerability, the Supplier must implement appropriate technical and organisational measures to mitigate the risk posed by the vulnerability.

# **Cloud Security Principles**

## The Supplier must ensure that the Supplier Solution complies with the Cloud Security Principles.

## The Supplier must assess the Supplier Solution against the Cloud Security Principles to assure itself that it complies with Paragraph 10.1:

### before Processing Government Data;

### at least once each Contract Year; and

### when required by the Buyer.

## The Supplier must:

### keep records of any assessment that it makes under Paragraph 10.2; and

### provide copies of those records to the Buyer within 10 Working Days of any request by the Buyer.

# **Information about Subcontractors, Sites, Third Party Tools and third parties**

## The Supplier must keep the following records:

### for Subcontractors or third parties that store, have access to or Process Government Data:

#### the Subcontractor or third party’s name:

##### legal name;

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

##### registration details (where the Subcontractor is not an individual), including:

###### country of registration;

###### registration number (if applicable); and

###### registered address;

#### the Relevant Certifications held by the Subcontractor or third party;

#### the Sites used by the Subcontractor or third party;

#### the Services provided or activities undertaken by the Subcontractor or third party;

#### the access the Subcontractor or third party has to the Supplier System;

#### the Government Data Processed by the Subcontractor or third party; and

#### the measures the Subcontractor or third party has in place to comply with the requirements of this Schedule 8 (*Security Management*);

### for Sites from or at which Government Data is accessed or Processed:

#### the location of the Site;

#### the operator of the Site, including the operator’s:

##### legal name;

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

##### registration details (where the Subcontractor is not an individual);

#### the Relevant Certifications that apply to the Site;

#### the Government Data stored at, or Processed from, the site; and

### for Third Party Tools:

#### the name of the Third Party Tool;

#### the nature of the activity or operation performed by the Third-Party Tool on the Government Data; and

#### in respect of the entity providing the Third-Party Tool, its:

##### full legal name;

##### trading name (if any)

##### country of registration;

##### registration number (if applicable); and

##### registered address.

## The Supplier must update the records it keeps in accordance with Paragraph 11.1:

### at least four times each Contract Year;

### whenever a Subcontractor, third party that accesses or Processes Government Data, Third Party Tool or Site changes; or

### whenever required to go so by the Buyer.

## The Supplier must provide copies of the records it keeps in accordance with Paragraph 11.1 to the Buyer within 10 Working Days of any request by the Buyer.

# **Encryption**

## The Supplier must, and must ensure that all Subcontractors, encrypt Government Data:

### when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and

### when transmitted.

# **Protective monitoring system**

## The Supplier must, and must ensure that Subcontractors, implement an effective system of monitoring and reports, analysing access to and use of the Supplier System and the Government Data to:

### identify and prevent any potential Breach of Security;

### respond effectively and in a timely manner to any Breach of Security that does;

### identify and implement changes to the Supplier System to prevent future any Breach of Security; and

### help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier System,

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

## The Protective Monitoring System must provide for:

### event logs and audit records of access to the Supplier System; and

### regular reports and alerts to identify:

#### changing access trends;

#### unusual usage patterns; or

#### the access of greater than usual volumes of Government Data; and

### the detection and prevention of any attack on the Supplier System using common cyber-attack techniques.

# **Patching**

## The Supplier must, and must ensure that Subcontractors, treat any public releases of patches for vulnerabilities as follows:

### the Supplier must patch any vulnerabilities classified as “critical”:

#### if it is technically feasible to do so, within 5 Working Days of the public release; or

#### if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 14.1(a)(i), then as soon as reasonably practicable after the public release;

### the Supplier must patch any vulnerabilities classified as “important”:

#### if it is technically feasible to do so, within 1 month of the public release; or

#### if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 14.1(b)(i), then as soon as reasonably practicable after the public release;

### the Supplier must remedy any vulnerabilities classified as “other” in the public release:

#### if it is technically feasible to do so, within 2 months of the public release; or

#### if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 14.1(c)(i), then as soon as reasonably practicable after the public release;

### where it is not technically feasible to patch the vulnerability, the Supplier must implement appropriate technical and organisational measures to mitigate the risk posed by the vulnerability.

# **Malware protection**

## The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier System.

## The Supplier must ensure that such Anti-virus Software:

### prevents the installation of the most common forms of Malicious Software in the Supplier System;

### performs regular scans of the Supplier System to check for Malicious Software; and

### where Malicious Software has been introduced into the Supplier System, so far as practicable

#### prevents the harmful effects from the Malicious Software; and

#### removes the Malicious Software from the Supplier System.

# **End-user Devices**

## The Supplier must, and must ensure that all Subcontractors, manage all End-user Devices on which Government Data is stored or processed in accordance with the following requirements:

### the operating system and any applications that store, process or have access to Government Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;

### users must authenticate before gaining access;

### all Government Data must be encrypted using a suitable encryption tool;

### 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;

### 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 Government Data to ensure the security of that Government Data;

### the Suppler or Subcontractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Government Data stored on the device and prevent any user or group of users from accessing the device;

### all End-user Devices are within the scope of any required Certification.

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

# **Vulnerability scanning**

## The Supplier must:

### scan the Supplier System at least once every month to identify any unpatched vulnerabilities; and

### if the scan identifies any unpatched vulnerabilities, ensure they are patched in accordance with Paragraph 14.

# **Access control**

## The Supplier must, and must ensure that all Subcontractors:

### identify and authenticate all persons who access the Supplier System before they do so;

### require multi-factor authentication for all user accounts that have access to Government Data or that are Privileged Users;

### allow access only to those parts of the Supplier System and Sites that those persons require;

### maintain records detailing each person’s access to the Supplier System.

## The Supplier must ensure, and must ensure that all Subcontractors ensure, that the user accounts for Privileged Users of the Supplier Information Management System:

### are allocated to a single, individual user;

### are accessible only from dedicated End-user Devices;

### are configured so that those accounts can only be used for system administration tasks;

### require passwords with high complexity that are changed regularly;

### automatically log the user out of the Supplier System after a period of time that is proportionate to the risk environment during which the account is inactive; and

### are:

#### restricted to a single role or small number of roles;

#### time limited; and

#### restrict the Privileged User’s access to the internet.

# **Return and deletion of Government Data**

## When requested to do so by the Buyer, the Supplier must, and must ensure that all Subcontractors:

### securely erase any or all Government Data held by the Supplier or Subcontractor using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted; or

### provide the Buyer with copies of any or all Government Data held by the Supplier or Subcontractor using the method specified by the Buyer.

# **Physical security**

## The Supplier must, and must ensure that Subcontractors, store the Government Data on servers housed in physically secure locations.

# **Breach of security**

## If the Supplier becomes aware of a Breach of Security that impacts or has the potential to impact the Government Data, it shall:

### notify the Buyer as soon as reasonably practicable after becoming aware of the breach, and in any event within [24] hours.

### provide such assistance to the Buyer as the Buyer requires until the Breach of Security and any impacts or potential impacts on the Buyer are resolved to the Buyer’s satisfaction.

### where the Law requires the Buyer to report a Breach of Security to the appropriate regulator provide such information and other input as the Buyer requires within the timescales specified by the Buyer.

# **Security Management Plan**

## This Paragraph 22 applies only where the Buyer has selected this option in paragraph 1.3.

1. *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 Supplier solution and the Buyer data.

## The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Agreement, the Security Management Plan, which must include a description of how all the options selected in this schedule are being met along with evidence of the required certifications for the Supplier and any Subcontractors specified in Paragraph 3.

1. *Approval of Security Management Plan*

## 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 operate the service and 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 10 Working Days of the date of the rejection, or such other period agreed with the Buyer.

## The rejection by the Buyer of a revised Security Management Plan is a material Default of this Agreement.

1. *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.

1. *Monitoring*

## The Supplier shall notify the Buyer within 2 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;

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