

# G-Cloud 13 Call-Off Contract

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

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

Part A: Order Form 2

Part B: Terms and conditions 15

Schedule 1: Services 36

Schedule 2: Call-Off Contract charges 37

Schedule 3: Collaboration agreement 38

Schedule 4: Alternative clauses 51

Schedule 5: Guarantee 56

Schedule 6: Glossary and interpretations 65

Schedule 7: UK GDPR Information 83

Annex 1: Processing Personal Data 84

Annex 2: Joint Controller Agreement 89

# 

# Part A: Order Form

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

|  |  |
| --- | --- |
| **Platform service ID number** | 428216402765823 |
| **Call-Off Contract reference** | CCZN23A10 |
| **Call-Off Contract title** | Provision of Hosting, Infrastructure and Single Sign On for ResilienceDirect |
| **Call-Off Contract description** | The ResilienceDirect™ team (RD), are seeking a provider Hosting, Infrastructure, Single Sign On & a Managed Service including 24/7 security monitoring and monthly and ad-hoc patching for the ResilienceDirect service and applications. ResilienceDirect™ is the UK’s free-to-use, secure web-based service for all Category 1 & 2 responders, government departments and other key organisations in the UK resilience community to share information during emergency responses, planning and exercises. The Service has in excess of 105,000 registered users and comprises of a number of applications. |
| **Start date** | 01 July 2023 |
| **Expiry date** | 30 June 2024 |
| **Call-Off Contract value** | Year 1 £621,000.00 per annum Year 2 (If extended) £626,400.00per annum. The total contract value including any extension options £ 1,247,400.00 |
| **Charging method** | Payment will be made on approval of invoice via BACS |
| **Purchase order number** | **REDACTED TEXT under FOIA Section 43 Commercial Interests.** |

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

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

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

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

|  |  |
| --- | --- |
| **From the Buyer** | Cabinet Office  **REDACTED TEXT under FOIA Section 40, Personal Information.** |
| **To the Supplier** | ANS  **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 **1st July 2023** and is valid for one (1) year period with the option to extend for up to twelve (12) months. (1+1) |
| **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).  18.1 of the Call Off Terms does not apply. |
| **Extension period** | This Call-Off Contract can be extended by the Buyer for **one** period of up to 12 months, by giving the Supplier **Four (4) 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 1: Cloud hosting |
| **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:   * **Schedule 1: Services** |
| **Additional Services** | Not applicable |
| **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 **as per Schedule 1.** |
| **Technical Standards:** | The service level and availability criteria required for this Call-Off Contract are **as per Schedule 1** |
| **Service level agreement:** | The service level and availability criteria required for this Call-Off Contract are **as per Schedule 1** |
| **Onboarding** | The onboarding plan for this Call-Off Contract is **as per Schedule 1.** |

|  |  |
| --- | --- |
| **Offboarding** | The offboarding plan for this Call-Off Contract is **as per Schedule 1.** |
| **Collaboration agreement** | Not applicable |
| **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 Call-Off Contract Term (whichever is the greater).  The annual total liability for all other defaults will not exceed the greater of in year 1 £621,000.00 (Six Hundred and Twenty-One Thousand Pounds) and Year 2 £ £626,400.00 (Six Hundred, Twenty-Six Thousand and Four Hundred 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 higher limit the Buyer requires (and as required by Law) |
| **Insurance** | The Supplier insurance(s) required will be:  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 higher limit the Buyer requires (and as required by Law) |
| **Buyer’s responsibilities** | **N/A** |
| **Buyer’s equipment** | **N/A** |

### Supplier’s information

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

### Call-Off Contract charges and payment

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

|  |  |
| --- | --- |
| **Payment method** | The payment method for this Call-Off Contract is BACS. |
| **Payment profile** | 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** | Invoices will be sent to **REDACTED TEXT under FOIA Section 43 Commercial Interests.** |
| **Invoice information required** | All invoices must include the month the service refers to and the current Purchase Order |
| **Invoice frequency** | Invoice will be sent to the Buyer monthly |
| **Call-Off Contract value** | The total value of this Call-Off Contract is £ £1,247,400. (excluding VAT) |
| **Call-Off Contract charges** | The breakdown of the Charges can be found in **Schedule 2: Call-Off Contract charges** |

### Additional Buyer terms

|  |  |
| --- | --- |
| **Performance of the** **Service** | The performance of the Services shall be pursuant of the ANS Managed Secure Cloud Service Definition (embedded).  ANS-SDD-Managed-Secure-Cloud (1).pdf |
| **Guarantee** | N/A |
| **Warranties, representations** | N/A |
| **Supplemental requirements in addition to the Call-Off** **terms** | N/A |
| **Alternative clauses** | N/A |
| **Buyer specific**  **amendments**  **to/refinements of the Call-Off Contract terms** | N/A |
| **Personal Data and** **Data Subjects** | Schedule 7 is being used in Annex 1. |
| **Intellectual Property** | N/A |
| **Social Value** | N/A |

### 1. Formation of contract

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

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

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

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

### 2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.13.

|  |  |  |
| --- | --- | --- |
| **Signed** | Supplier | Buyer |
| **Name** | **REDACTED TEXT under FOIA Section 40, Personal Information.** | **REDACTED TEXT under FOIA Section 40, Personal Information.** |
| **Title** | **REDACTED TEXT under FOIA Section 40, Personal Information.** | **REDACTED TEXT under FOIA Section 40, Personal Information.** |
| **Signature** | **REDACTED TEXT under FOIA Section 40, Personal Information.** | **REDACTED TEXT under FOIA Section 40, Personal Information.** |
| **Date** | **REDACTED TEXT under FOIA Section 40, Personal Information.** | **REDACTED TEXT under FOIA Section 40, Personal Information.** |

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](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

# THE REQUIREMENT

* 1. The following are mandatory Cloud Software requirements:
     1. The ResilienceDirect services must be accessible by the user community 24/7/365 with any exceptions or downtime being agreed in advance with the Authority.
     2. The System must be suitable for hosting OFFICIAL (Tier 1) including data with the handling data caveat OFFICIAL-SENSITIVE.
     3. The service provider must be UK based. This is in order to meet the security requirements of a large user community in which data sovereignty is a concern and therefore must apply system wide. The ResilienceDirect platform must be hosted in one of the Government Data Centre that is registered with the Home Office as a Police Assured Server Facility (PASF). Also, the Disaster Recovery facility must be in a second Data Centre within the scope of the PASF.
     4. The location of the Services will be carried out at both the supplier’s premises, and the Resilience Directorate team’s office Street 70 Whitehall Westminster, London.
     5. The services provided shall be delivered in accordance with the NCSC Cloud Security Principles: [https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-](https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles) [principles](https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles). The supplier is to provide a summary as to how their proposed service meets these requirements.
     6. The Supplier must ensure that they adhere to data protection legislation and GDPR regulations.
     7. The three environments are as follows: UAT, Production & Disaster Recovery.
     8. The Disaster Recovery Environment to be a separate infrastructure able to provide the same services as the Production Environment.
     9. The Supplier is to provide the support and process for the movement of Virtual Machines from UAT to PROD environments in support of the application development.
     10. The required service must have the capacity to increase the available resources as required to support future applications and the growth of the data and user communities.
     11. The Hosting supplier will need to work closely with the other three ResilienceDirect Suppliers.
     12. The following are mandatory Cloud Hosting requirements
     13. Infrastructure to be provided that will host the Virtual Machines as presented in Table 1.
     14. The PROD Infrastructure must be expandable to cope with increased community size, additional services/applications and to remedy potential performance issues. The supplier is to explain the process and time required for such changes and confirm any cost impacts.
     15. The Disaster recovery infrastructure must be capable of expanding the capacity when required to host additional services/applications. The process and time required for such changes are to be described by the supplier along with any limitations or ceilings that the Authority should consider.
     16. A Disaster Recovery infrastructure is required that will host the Virtual Machines identified as ’PROD’ in Table 1.
     17. If the Production system fails, a switch over to the Disaster Recovery environment should occur immediately with minimal or no loss of data. The supplier is to advise as to the RTO/RPO that can be achieved with the proposed DR service.
     18. The supplier is to provide details of the Business Continuity approach including the Service Level Agreement offered for the Disaster Recovery service and the subsequent restoration of the Production system.
     19. The required storage volume at the commencement of the contract is 40 TB for the Production system.
     20. Capacity for additional storage is to be provided, with the growth rate of data being in the order of 6TB per year.
     21. The infrastructure must support the ability to switch off/sleep individual virtual machines when they are not in use and turn on when required;
     22. The infrastructure must support the re-allocation of available compute and storage resources within the overall scope defined in Table 1.
     23. The Supplier will be responsible for the patching and maintenance of the infrastructure up to and including the operating systems of the application virtual machines. The patching does exclude 3rd party applications and middleware installed on the Operating systems – this responsibility remains with the application providers.
     24. All critical security patches are to be applied within 24 hours of the release of the details of the patch or configuration change.
     25. The standard patching cycle shall be no longer than one month.
     26. The infrastructure and all data stored within any element of the system (including DR and backups) must be located within the UK.
     27. The Supplier is to provide a backup solution for the infrastructure, that provides as a minimum, the ability to restore virtual machines with an RPO of no more than 24 hours (e.g. full weekly and daily incremental backups). This is to apply to all environments (UAT, PROD) and DR where required dependent upon the DR solution proposed.
     28. At least one copy of the backups is to be stored in a suitable secure location that is physically separate from the Production system. These ‘off-site’ backups to be no more than 1 week old.
     29. The Supplier will be required to provide additional backups and confirmation that backups have been successfully completed in support of the application development work undertaken by other RD suppliers.
     30. The Infrastructure shall place no size restrictions upon data uploaded/downloaded from the system.
     31. The supplier is to provide details of the process for increases in storage and time required.
  2. The following are mandatory Cloud Software requirements:
     1. The hosted applications require the ability to send outbound email for notifications. The supplier is to provide a mail relay facility to forward the email notifications from the applications using a single URL (mail.resilience.gov.uk) domain address.
     2. The mail relay must support the SPF, DKIM, DMARC configuration as recommended in the HMG guidance available at: [https://www.gov.uk/guidance/set-up-government-email-services-](https://www.gov.uk/guidance/set-up-government-email-services-securely) [securely](https://www.gov.uk/guidance/set-up-government-email-services-securely)
     3. The supplier is to provide and manage a Single Sign On service to authenticate all ResilienceDirect Users. This SSO service must integrate with each of the hosted applications to provide a single authentication across the service.
     4. The supplier is to provide documentation on how to use and integrate with the SSO solution such that future applications can be supported.
     5. The supplier must maintain and update the SSO service throughout the contractual period.
     6. The SSO service must support Multi-Factor authentication with two alternative options for authenticating email and a mobile app.
     7. The SSO service must provide reporting on authentication, both successful and failed authentication attempts.
     8. The SSO service must have a configurable password policy and session policies including maximum session time.
     9. Due to the number of applications hosted on the application, the Authority require a single Validation Multi-Domain SSL Certificate to be provided by the supplier. The Authority will provide the list of SANs to be included within the reslience.gov.uk domain certificate in addition to those required by the supplier. The Authority will provide the required domain authorisation to support as the domain owner.
     10. The supplier is responsible for the availability, integrity and confidentiality of the cloud software services provided by the supplier.
     11. The supplier must provide a secure method of remote access onto the application servers for the nominated application administrators.
     12. The remote access to the application servers must use secure keys as part of a multi-factor authentication process.
     13. It must be possible to restrict remote access to specified source IP addresses of the application vendors.
     14. Provide CO RD access to the monitoring dashboard based on CO specified IP addresses
     15. The supplier must provide logging and reports of Administrative access to all elements of the infrastructure, including the remote access server(s).
     16. The supplier shall provide and support Load Balancers for the Collaborate and Mapping applications and any infrastructure required by the SSO solution and will work with the other suppliers to maintain and integrate.
     17. The supplier shall provide a centrally managed AntiVirus and Anti Malware (AV) solution for all Virtual Machines listed in Table 1.
     18. The AV service shall include the distribution of updated AV libraries and profiles across the estate with updates being at least daily.
     19. The provision of software for the management, monitoring and audit of the service is to be included by the Supplier (to meet the Cloud Support requirements in the next section)
  3. The following are mandatory Cloud support requirements:
     1. The system shall achieve an availability of at least 99.97%. The supplier will be expected to work closely with other ResilienceDirect suppliers to ensure optimum service levels are maintained.
     2. The supplier shall advise the Authority and their suppliers of any planned maintenance activities at least 1 week in advance.
     3. The Supplier will be required to attend bi-weekly service review meetings with the Authority.
     4. The Supplier will be required to attend the bi-weekly RD Partners call, taking the chairmanship role in rotation with the other RD partners. The Supplier’s attendance at these meetings will be with representation that can present any planned work and understand the potential impact of work planned by the other RD suppliers.
     5. The Supplier shall attend the monthly security working group meetings, providing a representative that can contribute to the assessment of the current security posture and support the continuous improvement of the security of the system, its operating procedures and the evolving threats.
     6. The supplier is to take an active role in the ResilenceDirect supplier community offering technical and security advice to the Authority and

the other suppliers to the ResilienceDirect platform. A partnership approach is expected both with the Authority and the associated suppliers.

* + 1. The Supplier is to provide a Protective Monitoring service that meets the guidelines from NCSC on protective monitoring based on the threat modelling and 10 Steps to Cyber Security guidance.
    2. The Supplier is to provide health and capacity monitoring of the infrastructure, providing alerts and notification messages to the Authority and their suppliers for important and critical issues that may impact on the availability of the service.
    3. The Supplier is responsible for taking proactive measures based on the health and capacity monitoring to ensure the system availability targets are met, and to provide advice and recommendations to the Authority to improve the service resilience and availability.
    4. The Supplier is responsible for taking proactive measures based on the health and capacity monitoring to ensure the system availability targets are met, and to provide advice and recommendations to the Authority to improve the service resilience and availability.
    5. The Supplier is responsible for taking proactive measures based on the health and capacity monitoring to ensure the system availability targets are met, and to provide advice and recommendations to the Authority to improve the service resilience and availability.
    6. The Supplier is to provide is to provide SQL patching via the WSUS server.
    7. A supplier to arrange for the automation of Linux Patch downloads and distribution.
    8. The supplier will be required to support the Authorities CO security risk assessment process covering the ResilienceDirect technology, people and process. This will take the form of an annual assessment, followed by monthly review meetings and the proposal and implementation of remedial actions where identified, in addition to attendance at quarterly Security Governance meetings along with all other ResilienceDirect suppliers.
    9. The Authority will also arrange annual IT Security Health Checks (ITSHC)s to be undertaken by qualified 3rd parties which will include reviews of the infrastructure. The supplier is to provide the support needed, including granting access permissions and physical access where necessary to the infrastructure such that this testing can take place. The supplier is also required to attending the subsequent review meetings and the proposal and implementation of remedial actions where identified for any IT Security Health Checks undertaken that identify security issues that fall within the scope of supply.
    10. The IP addresses and URLs of the ResilienceDirect platform are registered with the NCSC Early Warning System (EWS). The Supplier will be responsible for this registration and the review of the security reports generated from it.
    11. The supplier will be required to ‘integrate’ their service desk tools for the management of incidents and problems with the ResilienceDirect first line support tool and the associated processes provided by Resilience Planning Services Ltd
    12. The supplier shall provide a service support tool for the management of incidents and problems that can be used by the Authority and the ResilienceDirect suppliers to raise service requests.
    13. The supplier shall provide a service support tool for the management of incidents and problems that can be used by the Authority and the ResilienceDirect suppliers to raise service requests.
    14. The supplier is to provide details of the Service Level Agreement being offered to the Authority.
    15. The current provider would export the existing VMs in an VMware OVF format – the supplier is to confirm that this method of service transition is supported.
    16. Provide details of the expectations for service transfer from the existing service provider and the timescales expected to restore the service.
    17. The supplier is to provide a tool for alerting for P1 (and P2) incidents and liaise with Authority's support desk, other suppliers and application owners.
    18. Table 1: Virtual machines listed

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **VM ID** | **Environment** | **vCPU**  **Cores** | **Memory (GB)** | **O/S** | **Comments** |
| COL1 | PROD | 2 | 16 | Windows Server | C |
| Media1 | PROD | 6 | 8 | Windows Server | Media Storage Server (5TB) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COL3 | PROD | 8 | 32 | Windows Server | MS SQL |
| COL4 | PROD | 8 | 32 | Windows Server | MS SQL |
| COL5 | PROD | 8 | 32 | Windows Server |  |
| COL6 | PROD | 8 | 32 | Windows Server |  |
| JOL1 | PROD | 4 | 16 | Windows Server |  |
| MAPS1 | PROD | 4 | 4 | Linux |  |
| MAPS2 | PROD | 4 | 12 | Linux |  |
| MAPS3 | PROD | 4 | 32 | Linux |  |
| MAPS4 | PROD | 4 | 32 | Linux |  |
| MAPS5 | PROD | 2 | 4 | Linux |  |
| MAPS6 | PROD | 4 | 32 | Linux |  |
| MAPS7 | PROD | 4 | 16 | Linux |  |
| MAPS8 | PROD | 4 | 8 | Linux |  |
| MAPS9 | PROD | 4 | 8 | Linux |  |
| MAPS10 | PROD | 2 | 4 | Linux |  |
| MAPS11 | PROD | 2 | 4 | Linux |  |
| MAPS12 | PROD | 4 | 16 | Linux |  |
| MAPS13 | PROD | 4 | 16 | Linux |  |
| MAPS14 | PROD | 4 | 16 | Linux |  |
| MAPS15 | PROD | 4 | 16 | Linux |  |
| MAPS16 | PROD | 4 | 16 | Linux |  |
| MAPS17 | PROD | 4 | 16 | Linux |  |
| MAPS18 | PROD | 4 | 16 | Linux |  |
| DASH1 | PROD | 2 | 4 | Linux |  |
| INFRA1 | PROD | 2 | 4 | Windows Server | Active Directory Server |
| INFRA2 | PROD | 4 | 12 | Windows Server |  |
| INFRA3 | PROD | 2 | 2 | Linux |  |
| INFRA4 | PROD | 2 | 2 | Linux |  |
| INFRA5 | PROD | 4 | 4 | Linux |  |
| INFRA6 | PROD | 4 | 4 | Linux | SSH Server for remote access by the application providers. |
| INFRA7 | PROD | 4 | 4 | Linux |  |
| SSO1 | PROD | 2 | 8 | Linux |  |
| SSO2 | PROD | 2 | 8 | Linux |  |
| SSO3 | PROD | 2 | 4 | Linux |  |
| SSO4 | PROD | 1 | 2 | Linux |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SSO1 | PROD | 4 | 8 | Linux |  |
| SSO2 | PROD | 4 | 8 | Linux |  |
| SSO3 | PROD | 2 | 4 | Linux |  |
| SSO4 | PROD | 4 | 8 | Linux |  |
| SSO5 | PROD | 2 | 4 | Linux |  |
| SSO6 | PROD | 4 | 8 | Linux |  |
| UAT MAPS1 | UAT | 2 | 4 | Linux |  |
| UAT MAPS2 | UAT | 4 | 16 | Linux |  |
| UAT MAPS3 | UAT | 4 | 16 | Linux |  |
| UAT MAPS4 | UAT | 4 | 16 | Linux |  |
| UAT MAPS5 | UAT | 4 | 16 | Linux |  |
| UAT MAPS6 | UAT | 2 | 4 | Linux |  |
| UAT MAPS7 | UAT | 2 | 4 | Linux |  |
| UAT MAPS8 | UAT | 4 | 12 | Linux |  |
| UAT DASH | UAT | 4 | 12 | Linux |  |
| INFRA1 | UAT | 4 | 4 | Linux | SSH Access Server |
| INFRA2 | UAT | 2 | 2 | Linux |  |
| INFRA3 | UAT | 2 | 2 | Linux | Proxy Server |
| INFRA4 | UAT | 4 | 4 | Linux | Mail Relay |
| INFRA5 | UAT | 4 | 4 | Linux |  |
| GLUU1 | UAT | 2 | 4 | Linux |  |
| GLUU2 | UAT | 2 | 8 | Linux |  |
| GLUU3 | UAT | 2 | 4 | Linux |  |
| GLUU4 | UAT | 1 | 2 | Linux |  |
| COL1 | UAT | 4 | 16 | Windows Server |  |
| COL2 | UAT | 4 | 16 | Windows Server |  |
| COL3 | UAT | 2 | 4 | Windows Server |  |
| COL4 | UAT | 4 | 16 | Windows Server |  |
| COL5 | UAT | 8 | 16 | Windows Server |  |
| COL6 | UAT | 8 | 16 | Windows Server |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| UAT- DOM01 | UAT | 2 | 8 | Windows Server |  |
| RD-UAT- RDMTZ1- MG01 | UAT | 2 | 4 | Windows Server |  |

* 1. The following are desirable Cloud Hosting requirements
     1. Disaster recovery and Business Continuity Plan to be shared and tested annually, with the participation of the Supplier and application owners.
  2. The following are desirable Cloud Software requirements
     1. The Supplier to engage application teams to understand changes going in as part of application release to ensure infrastructure is adequate in terms of resilience, performance and security.
     2. The supplier may be required to add further load balancers into the solution to support the hosted applications. The process, timescales and costs for doing so should be provided.
     3. Development work on the cloud software services may be requested by the Authority over the course of the service provision. Whilst such development is not expected to be within the scope of the supply, the supplier will not charge the Authority for the provision of the quotations and proposals.
     4. Provide CO RD access to the monitoring dashboard based on CO specified IP addresses.
  3. The following are desirable Cloud Support requirements:
     1. To explore the route from private cloud to public cloud and the changes needed to facilitate the migration, including applications, servers, current services used and security and access management.
     2. The supplier is to provide a tool for monitoring the health of the service, including suspicious activity in the infrastructure and

application. Supplier to liaise with the application owners to integrate this throughout the end to end and ensure that the firewall for ResilienceDirect can be configured to depict violation types and monitored and noted.

* + 1. The supplier is to maintain an awareness of the security vulnerabilities and vendor recommendations that relate to the infrastructure products proposed by the supplier. Information about how this knowledge is maintained will assist the Authority in assessing the suitability of the Supplier.

# KEY MILESTONES AND DELIVERABLES

* 1. 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 |
| 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. | Within week 1 of the Contract Award |
| 4 | Query response time.  Within 24 hours. Whether it be from the RD support desk or RD team, excluding weekends. If it is a | Within week 1 of the Contract Award |

|  |  |  |
| --- | --- | --- |
|  | priority 1 then the out of hours triage is activated and we expect a response within the hour. |  |
| 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. | Within week 1 of the Contract Award |
| 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 | Within week 1 of the Contract Award |

# MANAGEMENT INFORMATION/REPORTING

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

# VOLUMES

* 1. ResilienceDirect registered users have increased from 30,000 in 2018 to over 83,000 in March 2021 to currently over 105,000 in April 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.
  2. 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

* 1. The supplier will be expected to continually improve the way in which the required services are to be delivered throughout the contract duration.
  2. The Supplier should present new ways of working to the ResilienceDirect Team during weekly Contract service review meetings.
  3. 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.

* 1. The Supplier should present new ways of working to the Buyer during monthly Contract review meetings.
  2. 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

* 1. 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.
  2. The suppliers should ensure all staff are aware of social values and fully trained in inclusion and diversity laws and policies.

# QUALITY

* 1. The quality standards required for this Call-Off Contract are:
  2. ISO 27001:2013 - information security of our business operations and the data that is entrusted to the supplier.
  3. ISO 27017 provides information security controls that must be implemented, specifically relating to cloud services.
  4. 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.
  5. ISO 22301:2012 provides a framework for the continual maintenance and improvement of a business continuity management system.
  6. Cyber Essentials and Cyber Essential Plus government endorsed standard that demonstrates they have the five Cyber Essentials controls implemented.
  7. Adheres to the most current NCSC Security Guidelines - including the 14 Cloud Principles.
  8. NPPV3 Clearance for administration of Servers holding Police data.

# PRICE

The contract is capped to a maximum of £1,242,000.00 (at a maximum of £621,000.00 per annum for 1+1).

* 1. Prices are to be submitted to Resilience direct , via

email  [**REDACTED TEXT under FOIA Section 40, Personal Information.**](mailto:resiliencedirect@cabinetoffice.gov.uk) and including VAT and all other expenses relating to Contract delivery clearly highlighted.

# STAFF AND CUSTOMER SERVICE

* 1. The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.
  2. The Supplier’s staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.
  3. The Supplier shall ensure that staff understand the Buyer’s vision and objectives and will provide excellent customer service to the Buyer throughout the duration of the Contract.
  4. 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.

# SECURITY AND CONFIDENTIALITY REQUIREMENTS

* 1. All staff involved have SC clearance.
  2. The successful provider must adhere to National Cyber Security Centre security policies, ideally holding an industry security assurance certification;
  3. The service should be resilient to compromise from basic cyber-attacks such as commodity malware ingestion or OWASP vulnerability exploits;
  4. To implement the agreed recommendations from the ResilienceDirect risk assessment throughout contract lifecycle.
  5. Adhere to the security schedule in Annex A.

# PAYMENT AND INVOICING

* 1. Invoicing to be made calendar monthly in arrears.
  2. Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.
  3. Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.
  4. Invoices should be submitted to: **REDACTED TEXT under FOIA Section 40, Personal Information.**
  5. 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;
  6. The location of the Services will be carried out virtually and in both the supplier’s premises and CCS ResilienceDirect™ team’s office in **REDACTED TEXT under FOIA Section 40, Personal Information.**

# CONTRACT MANAGEMENT

* 1. Attendance at Contract Review meetings shall be at the Supplier’s own expense.
  2. The supplier will provide progress updates and clear actions as agreed during these meetings.
  3. The contract will commence on 1st July 2023 for 12 months, ending on 31st June 2024; 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.

# LOCATION

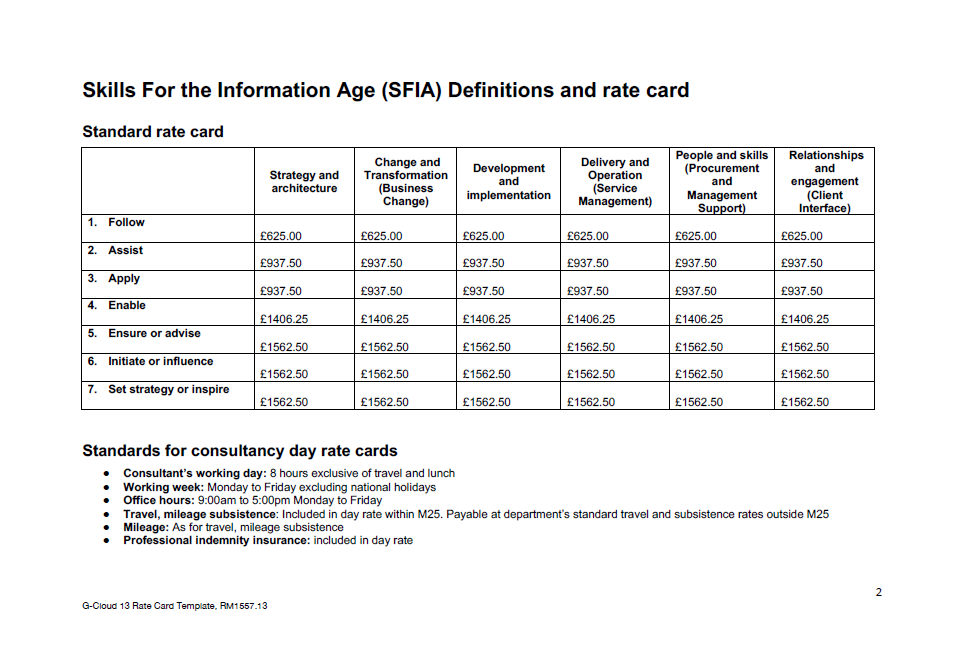
The location of the Services will be carried out at **REDACTED TEXT under FOIA Section 40, Personal Information.**

# SERVICE DESCRIPTION MANAGED SECURE CLOUD

ANS-SDD-Managed-Secure-Cloud (1).pdf

# 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:

Schedule 3 – 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: **REDACTED TEXT under FOIA Section 40, Personal Information.**

1.2 The contact details of the Supplier’s Data Protection Officer are: **REDACTED TEXT under FOIA Section 40, Personal Information.**

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 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. |

|  |  |
| --- | --- |
| Subject matter of the processing |  |
| Duration of the Processing | The processing is needed to ensure the processor can effectively provide a contingency platform. The processing includes basic login details of Resilience Direct administrators as well as a variety of personal information that may be input during the administration of a live contingency event. Joint controllers who use the platform will be responsible for creating privacy notices based on their own intended use. |
| Nature and purposes of the Processing | The collection of login data for administrators enables them to provide access to users within their own organisations, as well as carrying out audits |
| Type of Personal Data | Administrators:  User IDs (unique to the user)  Names - compulsory  Email addresses - compulsory  Telephone numbers - optional |

|  |  |
| --- | --- |
| Categories of Data Subject | Government employees and other first responders who might provide multi agency responses should a major incident be declared Members of the public who may be involved in such incidents  ResilienceDirect does not take ownership of any data uploaded to the platform.  No data is fully deleted from the  ResilienceDirect platform as it is kept for audit and enquiry purposes. |
| 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 | Returning information if the processor no longer holds the contract - is covered by the security schedule para 12 and 19 eg encryption when at rest or in transit and deleted at our request. |

Annex 2: NOT USED