Crown Commercial Service

G-Cloud 14 Call-Off Contract

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

G-Cloud 14 Call-Off Contract

Part A: Order Formsoftcat

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	138755276751549
Call-Off Contract reference	CO/IBCA/3662
Call-Off Contract title	IBCA SoftCat Case Management System
Call-Off Contract description	Contract for the provision of case management technology tool and associated training and support.
Start date	01 March 2025
Expiry date	28 February 2028
Call-Off Contract value	**The Contract value is up to £601,988.11 (£722,385.73 Including VAT)** Spend commitment beyond the initial Three Years (36 months) term is at the at the sole discretion of the Buyer. **REDACTED TEXT under FOIA Section 43 Commercial Interests.**
Charging method	Electronic Invoice
Purchase order number	To be confirmed upon contract signature

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

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

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

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

From the Buyer	**REDACTED TEXT under FOIA Section 40, Personal Information**. .
To the Supplier	Softcat plc Fieldhouse Lane, Marlow, Bucks, SL7 1LW Company number 02174990
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 01 March 2025 and is valid for **Three Years (36 months)**

Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least **90** Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause (as per clause 18.1). Such notice shall not be invoked in the first 36 months of the contract. The Commercial offer is submitted under the requirement for a full-term commitment from the Buyer.
Extension period	This Call-Off Contract can be extended by the Buyer for **One Year (12 months)** , by giving the Supplier **30 days** 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.

Buyer contractual details

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

G-Cloud Lot	This Call-Off Contract is for the provision of Services Under: Lot 2: Cloud software

G-Cloud Services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below: Lot 2: Cloud software
Additional Services	The Buyer may request additional services within the scope of Supplier's G-Cloud Service Offering. 1) Flowable AI-Studio 2) Flowable Whatsapp Connector 3) Additional Flowable Training
Location	Licencing and training will be delivered remotely
Quality Standards	The quality standards required for this Call-Off Contract are specified in GCloud 14 Framework, Call-Off Contract, Supplier's G-Cloud Offering and further detailed in Schedule 1 Services
Technical Standards:	The technical standards used as a requirement for this Call-Off Contract are specified in G-Cloud 14 Framework, Call-Off Contract, Supplier's G-Cloud Offers and further detailed in Schedule 1 Services. Supplier shall ensure that all Supplier's and Subcontractor's staff are assured to the UK Government Baseline Personnel Security Standard (BPSS) check and are security cleared (SC) level where necessary, prior to the ability to directly or indirectly access or influence Buyer systems or Buyer materials.
Service level agreement:	The service levels required for this contract are: As detailed in Annex 1 of the Maintenance and Support in the Flowable Subscription and Services Agreement, included within this call-off at Schedule 1: Services. The Service Level for the product support on the Flowable Platform software is GOLD and defined as following:

	Service Level Agreement — **GOLD** **SLA-relevant Support Channel** — Web-based Ticketing System **SLA-relevant Support Hours** — 24 x 7 x 365[1] **Authorized Support Contacts** — 3 **SLA-relevant Support Requests** — Incidents **Non-SLA-relevant Support Requests** — Questions, Change Request **SLA-relevant Support Time: Initial Response Time** **Severity One Incident** — 4h **Severity Two Incident** — 8h **Severity Three Incident** — 1 Business Day **Severity Four Incident** — 2 Business Days ***[1]*** *7 days a week and 365 days per year* ***[2]*** *7 days a week and 365 days per year*
Onboarding	The Parties will agree to the Implementation and Deployment of Licenses and Training as required within one week of valid Purchase Order.

Offboarding	The offboarding arrangements for this Call-Off Contract shall be jointly agreed by the Buyer and the Supplier 90 days before the Contract expiry date.

Collaboration agreement	A specific collaboration agreement is not required at this stage. The Supplier is expected to enter a collaboration agreement if required or to reasonably collaborate with the Buyer's third-party suppliers, appointed by the Buyer. The Supplier is expected to adopt the Buyer's protocols, local security protocols necessary to gain access to secure areas and agreed approaches to ensure synchronisation and integration with existing delivery teams as appropriate
Limit on Parties' liability	The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data will not exceed 125**%** of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). The annual total liability of the Supplier for all other 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 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract term.
Buyer's responsibilities	The Buyer is responsible for **compliance with Flowable Subscription and Services Agreement (SSA), included at Schedule 1: Services.**
Buyer's equipment	N/A

Supplier's information

Subcontractors or partners	Trading Name(s): Flowable AG Company Number: CHE-105.136.021 Registered Address(ees) and Contact Details: Weltpoststrasse 5, CH-3015 Bern Goods/Services to be provided: Flowable Platform Subscription, Flowable Training, Flowable Professional Services

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 by Electronic Bank Transfer (BACS).
Payment profile	Annual in Advance.
Invoice details	The Supplier will issue electronic invoices as per the payment profile. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to	Invoices will be sent to accounts payable. **REDACTED TEXT under FOIA Section 40, Personal Information**.
Invoice information required	All invoices must include the purchase order number, contract reference number CO/IBCA/3662, a summary of the contracted services. All invoices must comply with HMRC requirements for VAT invoices.
Invoice frequency	Invoicing frequency as per the payment profile.
Call-Off Contract value	The total value of this Call-Off Contract is **£601,988.11**

Call-Off Contract charges	**The Contract value is up to £601,988.11 (£722,385.73 Including VAT)** Spend commitment beyond the initial Three Years (36 months) term is at the at the sole discretion of the Buyer. **REDACTED TEXT under FOIA Section 43 Commercial Interests.**

Additional Buyer terms

Performance of the Service	As per Schedule 1: Services. This Call-Off Contract will include the following Implementation Plan: ● Licenses provided within 2 Working Days on signature and user accounts set-up ● All users to be trained, prior to CMS Solution go live.
Guarantee	Not used
Warranties, representations	In addition to the incorporated Framework Agreement clause 2.3, the Supplier warrants and represents to the Buyer that: ● the Supplier will perform its obligations under this Call-Off Contract with all reasonable care, skill and diligence, according to Good Industry Practice. ● the Supplier will not intentionally introduce disruptive elements into systems providing services to data, software or Authority Confidential Information held in electronic form. ● the Supplier undertakes to the Buyer that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Call-Off Contract Order Form.

	● the Supplier warrants that it has full capacity and authority and all necessary authorisations, consents, licences and permissions and Intellectual Property Rights to perform this Call-Off Contract. ● the Supplier represents that, in entering into this Call-Off Contract, it has not committed any Fraud. ● the Supplier undertakes to pay all taxes due from it to HMRC and will not indulge in “disguised employment” practices when delivering services under this Call-Off Contract, and For the avoidance of doubt, the fact that any provision within this Call-Off Contract is expressed as a warranty shall not preclude any right of termination the Buyer may have in respect of breach of that provision by the Supplier.
Supplemental requirements in addition to the Call-Off terms	● The Supplier will comply Schedule 10: Security and ensure compliance of Supplier’s Subcontractors as defined in Schedule 10. ● Schedule 10 Security Management has been included and covers ISO27001, Cyber Essentials plus, ISO22301 requirements. ● During the period of subscription for Flowable Work by Licensee, Licensee grants Licensor permission to display the Licensee logo on the Flowable website www.flowable.com under customer references.
Alternative clauses	Not used
Buyer specific amendments to/refinements of the Call-Off Contract terms	The Supplier will comply Schedule 10: Security and ensure compliance of Supplier’s Subcontractors as defined in Schedule 10.
Personal Data and Data Subjects	Schedule 7 Annex 1

Intellectual Property	Standard Framework and Call-Off contract IPR provisions.
Social Value	Social value commitments as per Supplier's G-Cloud Service Offering.
Performance Indicators	Data supplied by the Supplier in relation to Performance Indicators is deemed the Intellectual Property of the Buyer and may be published by mutual agreement between the Buyer and the Supplier. [Note required Performance Indicators needed from the Supplier for future publication or otherwise]

1. Formation of contract

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

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

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

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

2. Background to the agreement

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

Signed	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	[**Enter date**]	[**Enter date**]

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

Buyer Benefits

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

G-Cloud 14 Customer Benefit Record

Part B: Terms and conditions

1. Call-Off Contract Start date and length

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

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

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

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

2. Incorporation of terms

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

2.3 (Warranties and representations)

4.1 to 4.6 (Liability)

4.10 to 4.11 (IR35)

5.4 to 5.6 (Change of control)

5.7 (Fraud)

5.8 (Notice of fraud)

7 (Transparency and Audit)

8.3 to 8.6 (Order of precedence)

11 (Relationship)

14 (Entire agreement)

15 (Law and jurisdiction)

16 (Legislative change)

17 (Bribery and corruption)

18 (Freedom of Information Act)

19 (Promoting tax compliance)

20 (Official Secrets Act)

21 (Transfer and subcontracting)

23 (Complaints handling and resolution)

24 (Conflicts of interest and ethical walls)

25 (Publicity and branding)

26 (Equality and diversity)

28 (Data protection)

30 (Insurance)

31 (Severability)

32 and 33 (Managing disputes and Mediation)

34 (Confidentiality)

35 (Waiver and cumulative remedies)

36 (Corporate Social Responsibility)

paragraphs 1 to 10 of the Framework Agreement Schedule 3

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

- a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'
- a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'
- a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

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.

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

4.1.4 respond to any enquiries about the Services as soon as reasonably possible

4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer

4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.

4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.

4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.

4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.

4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14 digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

5.1 Both Parties agree that when entering into a Call-Off Contract they:

5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party

5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms

5.1.3 have raised all due diligence questions before signing the Call-Off Contract

5.1.4 have entered into the Call-Off Contract relying on their own due diligence

6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their Service Descriptions.

6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

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

7. Payment, VAT and Call-Off Contract charges

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

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

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

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

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

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

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

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

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

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

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

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

10. Confidentiality

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

11. Intellectual Property Rights

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

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

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

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

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

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

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

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

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

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

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

- rights granted to the Buyer under this Call-Off Contract
- Supplier's performance of the Services
- 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:

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

- the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract
- other material provided by the Buyer necessary for the Services

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

12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

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

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

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

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

13. Buyer data

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

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

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

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

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

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

13.6.1 the principles in the Security Policy Framework: https://www.gov.uk/government/publications/security-policy-framework and the Government Security - Classification policy: https:/www.gov.uk/government/publications/government-security-classifications

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

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

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

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

13.6.6 Buyer requirements in respect of AI ethical standards.

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

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

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

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

14. Standards and quality

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

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at: https://www.gov.uk/government/publications/technologycode-of-practice/technology -code-of-practice

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

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

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

15. Open source

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

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

16. Security

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

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

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

16.4 Responsibility for costs will be at the:

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

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

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

16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:
https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

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

17. Guarantee

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

17.1.1 an executed Guarantee in the form at Schedule 5

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

18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

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

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

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

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

18.4.2 any fraud

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

18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is

remediable, fails to remedy it within 15 Working Days of being notified in writing to do so

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses
7 (Payment, VAT and Call-Off Contract charges)
8 (Recovery of sums due and right of set-off)
9 (Insurance)
10 (Confidentiality)
11 (Intellectual property rights)
12 (Protection of information)

13 (Buyer data)
19 (Consequences of suspension, ending and expiry)
24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability),
24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

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

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

- return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
- return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
- 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
- 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
- work with the Buyer on any ongoing work
- return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

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.

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

20. Notices

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

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

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

21. Exit plan

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

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

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

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

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

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

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

21.6.2 there will be no adverse impact on service continuity

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

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

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

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

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

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

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

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

22. Handover to replacement supplier

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

23. Force majeure

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

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

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

24. Liability

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

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

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

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

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

24.4 When calculating the Supplier’s liability under Clause 24.1 any items specified in Clause

24.2 will not be taken into consideration.

25. Premises

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

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

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

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

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

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

25.5.2 comply with Buyer requirements for the conduct of personnel

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

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

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

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

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

29.2.1 the activities they perform
29.2.2 age
29.2.3 start date
29.2.4 place of work
29.2.5 notice period
29.2.6 redundancy payment entitlement
29.2.7 salary, benefits and pension entitlements
29.2.8 employment status
29.2.9 identity of employer
29.2.10 working arrangements

29.2.11 outstanding liabilities
29.2.12 sickness absence
29.2.13 copies of all relevant employment contracts and related documents
29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer.

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.

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.

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

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

- its failure to comply with the provisions of this clause
- 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
- The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.
- For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

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

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

31. Collaboration

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

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

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

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

32. Variation process

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

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

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

33. Data Protection Legislation (GDPR)

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

Schedule 1: Services

Licensed Software Flowable PLATFORM Product Description
Flowable Platform is a commercially licensed software that provides a complete case, process, task and content management capability; allowing for tailor made business process automation solutions. Flowable Platform includes the applications and functionality of Flowable Work, Flowable Design, Flowable Control and Flowable Inspect. Specific requirements are stated and published on: https://documentation.flowable.com/latest/admin/installs/platform-full **Flowable Work** is a commercially licensed software of Flowable Platform, that provides a business process workplace for users to interact with their case, process, form, document and other process data. In addition it allows users to access their activities from a dashboard configurable user experience and work with the business process solutions implemented on the Flowable Platform. Specific requirements are stated and published on: https://documentation.flowable.com/latest/admin/installs/platform-full **Flowable Design** is a commercially licensed software of Flowable Platform in the form of a graphical model designer. Flowable Design is a dynamic process design software used for developing case, process, form and other application models. It allows users to define models that can be executed within the Flowable Platform at runtime. Specific requirements are stated and published on: https://documentation.flowable.com/latest/admin/installs/design-quick **Flowable Control** is a commercially licensed software of Flowable Platform, in the form of an application for administration and monitoring of Flowable generated applications. Flowable Control allows users to fully monitor and manage their runtime environments. Specific requirements are stated and published on: https://documentation.flowable.com/latest/admin/installs/control-quick **Flowable Inspect** is a commercially licensed software of Flowable Platform, that provides functionality to debug and test process and case models under development. Flowable Inspect is a component of the Flowable Platform and it allows admin users to perform process test and debugging on a visual interface. Specific requirements are stated and published on: https://documentation.flowable.com/latest/admin/installs/platform-full

REDACTED TEXT under FOIA Section 43 Commercial Interests.

Schedule 2: Call-Off Contract charges

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

The Contract value is up to £601,988.11 (£722,385.73 Including VAT)

Spend commitment beyond the initial Three Years (36 months) term is at the at the sole discretion of the Buyer.

REDACTED TEXT under FOIA Section 43 Commercial Interests.

Schedule 3: Collaboration agreement - NOT USED

Schedule 4: Alternative clauses

1. Introduction

1.1 This Schedule specifies the alternative clauses that may be requested in the Order Form and, if requested in the Order Form, will apply to this Call-Off Contract.

2. Clauses selected

2.1 The Buyer may, in the Order Form, request the following alternative Clauses:

2.1.1 Scots Law and Jurisdiction

2.1.2 References to England and Wales in incorporated Framework Agreement clause 15.1 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.

2.1.3 Reference to England and Wales in Working Days definition within the Glossary and interpretations section will be replaced with Scotland.

2.1.4 References to the Contracts (Rights of Third Parties) Act 1999 will be removed in clause 27.1. Reference to the Freedom of Information Act 2000 within the defined terms for 'FoIA/Freedom of Information Act' to be replaced with Freedom of Information (Scotland) Act 2002.

2.1.5 Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.1.

2.1.6 References to "tort" will be replaced with "delict" throughout

2.2 The Buyer may, in the Order Form, request the following Alternative Clauses:

2.2.1 Northern Ireland Law (see paragraph 2.3, 2.4, 2.5, 2.6 and 2.7 of this Schedule)

2.3 Discrimination

2.3.1 The Supplier will comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular the:

- Employment (Northern Ireland) Order 2002
- Fair Employment and Treatment (Northern Ireland) Order 1998
- Sex Discrimination (Northern Ireland) Order 1976 and 1988
- Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003

- Equal Pay Act (Northern Ireland) 1970
- Disability Discrimination Act 1995
- Race Relations (Northern Ireland) Order 1997
- Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996
- Employment Equality (Age) Regulations (Northern Ireland) 2006
- Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000
- Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002
- The Disability Discrimination (Northern Ireland) Order 2006
- The Employment Relations (Northern Ireland) Order 2004
- Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006
- Employment Relations (Northern Ireland) Order 2004
- Work and Families (Northern Ireland) Order 2006

and will use its best endeavours to ensure that in its employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract it promotes equality of treatment and opportunity between:

- persons of different religious beliefs or political opinions
- men and women or married and unmarried persons
- persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)
- persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)
- persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)
- persons of different ages
- persons of differing sexual orientation

2.3.2 The Supplier will take all reasonable steps to secure the observance of clause 2.3.1 of this Schedule by all Supplier Staff.

2.4 Equality policies and practices

2.4.1 The Supplier will introduce and will procure that any Subcontractor will also introduce and implement an equal opportunities policy in accordance with guidance from and to the satisfaction of the Equality Commission. The Supplier will review these policies on a regular basis (and will procure that its Subcontractors do likewise) and the Buyer will be entitled to receive upon request a copy of the policy.

2.4.2 The Supplier will take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in clause 2.3 above). These steps will include:

- the issue of written instructions to staff and other relevant persons
- the appointment or designation of a senior manager with responsibility for equal opportunities
- training of all staff and other relevant persons in equal opportunities and harassment matters
- the inclusion of the topic of equality as an agenda item at team, management and staff meetings

The Supplier will procure that its Subcontractors do likewise with their equal opportunities policies.

2.4.3 The Supplier will inform the Buyer as soon as possible in the event of:

- the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or
- any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its Subcontractors during the Call-Off Contract Term by any Industrial or Fair Employment Tribunal or court,

The Supplier will take any necessary steps (including the dismissal or replacement of any relevant staff or Subcontractor(s)) as the Buyer directs and will seek the advice of the Equality Commission in order to prevent any offence or repetition of the unlawful discrimination as the case may be.

2.4.4 The Supplier will monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and will provide an annual report on the composition of the workforce and applicants to the Buyer. If the monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier will review the operation of its relevant policies and take positive action if appropriate. The Supplier will impose on its Subcontractors obligations similar to those undertaken by it in this clause 2.4 and will procure that those Subcontractors comply with their obligations.

2.4.5 The Supplier will provide any information the Buyer requests (including Information requested to be provided by any Subcontractors) for the purpose of assessing the Supplier's compliance with its obligations under clauses 2.4.1 to 2.4.5 of this Schedule.

2.5 Equality

2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant

agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

2.5.2 The Supplier acknowledges that the Buyer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours to assist (and to ensure that relevant Subcontractor helps) the Buyer in relation to same.

2.6 Health and safety

2.6.1 The Supplier will promptly notify the Buyer of any health and safety hazards which may arise in connection with the performance of its obligations under the Call-Off Contract. The Buyer will promptly notify the Supplier of any health and safety hazards which may exist or arise at the Buyer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Contract.

2.6.2 While on the Buyer premises, the Supplier will comply with any health and safety measures implemented by the Buyer in respect of Supplier Staff and other persons working there.

2.6.3 The Supplier will notify the Buyer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Buyer premises if that incident causes any personal injury or damage to property which could give rise to personal injury.

2.6.4 The Supplier will comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other persons working on the Buyer premises in the performance of its obligations under the Call-Off Contract.

2.6.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Buyer on request.

2.7 Criminal damage

2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Buyer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Buyer under any insurance policy).

2.7.2 If during the Call-Off Contract Term any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.

2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Buyer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Buyer's cost and the Supplier will (at no additional cost to the Buyer) provide any help the Buyer reasonably requires with the appeal.

2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

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-to-date version must be used. At the time of drafting the tool may be found here:

	https://www.gov.uk/guidance/check-employment-status-fortax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Financial Metrics	The following financial and accounting measures: Dun and Bradstreet score of 50 Operating Profit Margin of 2% Net Worth of 0 Quick Ratio of 0.7
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 RM1557.14 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.

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

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

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

Insolvency event	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 Supplier Trigger Event

Intellectual Property Rights or IPR	Intellectual Property Rights are: (a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information (b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction (c) 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, judgement of a relevant court of law, or directives or

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

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

Platform	The government marketplace where Services are available for Buyers to buy.
Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK GDPR.
Prohibited act	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 and Performance Indicators data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controlscheck-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or

	facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.

Supplier staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Trigger Event	The Supplier simultaneously fails to meet three or more Financial Metrics for a period of at least ten Working Days.

Variation	This has the meaning given to it in clause 32 (Variation process).
Variation Impact Assessment	An assessment of the impact of a variation request by the Buyer completed in good faith, including: details of the impact of the proposed variation on the Deliverables and the Supplier's ability to meet its other obligations under the Call-Off Contract; details of the cost of implementing the proposed variation; details of the ongoing costs required by the proposed variation when implemented, including any increase or decrease in the Charges, any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party; a timetable for the implementation, together with any proposals for the testing of the variation; and such other information as the Buyer may reasonably request in (or in response to) the variation request;
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Intentionally Blank

Schedule 7: UK GDPR Information

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

Annex 1 - Processing Personal Data

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

1.1.1.1 The contact details of the Buyer's Data Protection Officer are: **REDACTED TEXT under FOIA Section 40, Personal Information**.

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

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

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

Identity of Controller and Processor for each Category of Personal Data	Under the terms of this contract, Softcat will not be Processing any Buyer Personal Data under, save for the contract information enclosed. Therefore, Softcat cannot be considered to be the Data Processor. Flowable (the Supplier's Sub-contractor) will not have access to any Buyer Personal Data. The Parties acknowledge for the purposes of the Data Protection Legislation, the Buyer is the Controller.
Duration of the Processing	N/A
Nature and purposes of the Processing	N/A
Type of Personal Data	N/A

Categories of Data Subject	*N/A*
International transfers and legal gateway	Not applicable
Plan for return and destruction of the data once the Processing is complete	N/A

Annex 2 - Joint Controller Agreement

Joint Controller Status and Allocation of Responsibilities

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

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

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

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

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

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

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

1. Undertakings of both Parties

1.1.1.1 The Supplier and Buyer each undertake that they shall:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

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

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

(k) where the Personal Data is subject to UK GDPR, not transfer such Personal Data outside of the UK unless the prior written consent of the

non-transferring Party has been obtained and the following conditions are fulfilled:

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

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

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

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

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

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

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

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

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

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

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

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

2. Data Protection Breach

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

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

(b) all reasonable assistance, including:

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

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

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

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete

information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

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

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

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

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

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

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

3. Audit

1.1.3.1 The Supplier shall permit:

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

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

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

4. Impact Assessments

1.1.4.1 The Parties shall:

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

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

5. ICO Guidance

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

6. Liabilities for Data Protection Breach

[Guidance: This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

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

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

if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Buyer is responsible for, then

the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

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

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

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

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

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

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

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

7. Termination

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

8. Sub-Processing

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

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

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

9. Data Retention

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

Schedule 8 (Corporate Resolution Planning) - NOT USED

Schedule 9 - Variation Form

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

Contract Details		
This variation is between:	**[insert** name of Buyer] **("the Buyer")** And **[insert** name of Supplier**]** (**"the Supplier"**)	
Contract name:	**[insert** name of contract to be changed] **("the Contract")**	
Contract reference number:	**[insert** contract reference number]	
Details of Proposed Variation		
Variation initiated by:	**[delete** as applicable: Buyer/Supplier]	
Variation number:	**[insert** variation number]	
Date variation is raised:	**[insert** date]	
Proposed variation		
Reason for the variation:	**[insert** reason]	
A Variation Impact Assessment shall be provided within:	**[insert** number] days	
Impact of Variation		
Likely impact of the proposed variation:	**[Supplier to insert** assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: **[Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause]	
Financial variation:	Original Contract Value:	£ **[insert** amount]
	Additional cost due to variation:	£ **[insert** amount]
	New Contract value:	£ **[insert** amount]

This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by Buyer

Words and expressions in this Variation shall have the meanings given to them in the Contract.

The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the Buyer

Signature	.....
Date	.....
Name (in Capitals)	.....
Address	.....

.....

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

Signature	.....
Date	.....
Name (in Capitals)	.....
Address	.....

Schedule 10 - Security Management

1 SUPPLIER OBLIGATIONS

Core requirements

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

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

Certifications (see Paragraph 4)		
The Supplier must have the following Certifications (or equivalent):	ISO/IEC 27001:2022 by a UKAS-recognised Certification Body	☐
	Cyber Essentials Plus	☒
	Cyber Essentials	☐
	No certification required	☐
Subcontractors that Handle Government Data must have the following Certifications (or equivalent):	ISO/IEC 27001:2022 by a UKAS-recognised Certification Body	☐
	Cyber Essentials Plus	☐
	Cyber Essentials	☒
	No certification required	☐
Locations (see Paragraph 5)		
The Supplier and Subcontractors may store, access or Handle Government Data in:	the United Kingdom only	☐
	a location permitted by and in accordance with any regulations for the time being in force made under 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State)	☒

	anywhere in the world not prohibited by the Buyer	☐
Staff Vetting Procedure (see Paragraph 6)		
The Buyer requires a Staff Vetting Procedure other than BPSS		☐
Where an alternative Staff Vetting Procedure is required, the procedure is: [**Set out required Staff Vetting Procedure (other than BPSS)**]		

Optional requirements

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

Security Management Plan (see Paragraph 10)	
The Supplier must provide the Buyer with a Security Management Plan detailing how the requirements for the options selected in this table have been met.	☐
Buyer Security Policies (see Paragraph 11)	
The Buyer requires the Supplier to comply with the following policies relating to security management: ● [**List Buyer security policies with which the Supplier and Sub-contractors must comply**].	☐
Security testing (see Paragraph 12)	
The Supplier must undertake security testing at least once every Contract Year and remediate any vulnerabilities, where it is technically feasible to do so	☒
Cloud Security Principles (see Paragraph 13)	
The Supplier must assess the Supplier System against the Cloud Security Principles	☐
Record keeping (see Paragraph 14)	

The Supplier must keep records relating to Subcontractors, Sites, Third-Party Tools and third parties	☒
Encryption (see Paragraph 15)	
The Supplier must encrypt Government Data while at rest or in transit	☒
Protective Monitoring System (see Paragraph 16)	
The Supplier must implement an effective Protective Monitoring System	☒
Patching (see Paragraph 17)	
The Supplier must patch vulnerabilities in the Supplier System promptly	☒
Malware protection (see Paragraph 18)	
The Supplier must use appropriate Anti-virus Software	☒
End-User Devices (see Paragraph 19)	
The Supplier must manage End-User Devices appropriately	☒
Vulnerability scanning (see Paragraph 20)	
The Supplier must scan the Supplier System monthly for unpatched vulnerabilities	☒
Access control (see Paragraph 21)	
The Supplier must implement effective access control measures for those accessing Government Data and for Privileged Users	☒
Remote Working (see Paragraph 22)	
The Supplier may allow Supplier Staff to undertake Remote Working once an approved Remote Working Policy is in place	☒
Backup and recovery of Government Data (see Paragraph 23)	

The Supplier must have in place systems for the backup and recovery of Government Data	☒
Return and deletion of Government Data (see Paragraph 24)	
The Supplier must return or delete Government Data when requested by the Buyer	☒
Physical security (see Paragraph 25)	
The Supplier must store Government Data in physically secure locations	☒
Security breaches (see Paragraph 26)	
The Supplier must report any Breach of Security to the Buyer promptly	☒

2 DEFINITIONS

[Guidance: the defined term 'Government Date' used within this Annex can be found within Clause 1 (Definitions used in the Contract).

"Anti-virus Software" means software that:

(a) protects the Supplier System from the possible introduction of Malicious Software;

(b) scans for and identifies possible Malicious Software in the Supplier System;

(c) if Malicious Software is detected in the Supplier System, so far as possible:

(i) prevents the harmful effects of the Malicious Software; and

(ii) removes the Malicious Software from the Supplier System;

"BPSS" means the employment controls applied to any individual member of the Supplier Staff that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 7.0, June 2024 (https://www.gov.uk/government/publications/government-baseline-personnel-security-standard), as that document is updated from time to time;

"Breach of Security" means the occurrence of:

(a) any unauthorised access to or use of the Services, the Sites, the Supplier System and/or the Government Data;

(b) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any Government Data, including copies of such Government Data; and/or

(c) any part of the Supplier System ceasing to be compliant with the required Certifications;

(d) the installation of Malicious Software in the Supplier System:

(e) any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the Supplier System; and

(f) includes any attempt to undertake the activities listed in sub-Paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:

(i) was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or

(ii) was undertaken, or directed by, a state other than the United Kingdom;

"Buyer Equipment"	means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System;
"Buyer Security Policies"	means those securities specified by the Buyer in Paragraph 1.3;
“Buyer System”	means the Buyer's information and communications technology system, including any software or Buyer Equipment, owned by the Buyer or leased or licenced to it by a third-party, that: (a) is used by the Buyer or Supplier in connection with this Contract; (b) interfaces with the Supplier System; and/or (c) is necessary for the Buyer to receive the Services.
“Certifications”	means one or more of the following certifications (or equivalent): (a) ISO/IEC 27001:2022 by a UKAS- recognised Certification Body in respect of the Supplier System, or in respect of a wider system of which the Supplier System forms part; and (b) Cyber Essentials Plus; and/or (c) Cyber Essentials;
“CHECK Scheme”	means the NCSC’s scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks;
“CHECK Service Provider”	means a company which, under the CHECK Scheme: (a) has been certified by the NCSC; (b) holds “Green Light” status; and (c) is authorised to provide the IT Health Check services required by Paragraph 9.2 (*Security Testing*);
“Cloud Security Principles”	means the NCSC’s document “Implementing the Cloud Security Principles” as updated or replaced from time to time and found at

	https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles;
"Contract Year"	means: 14.9.1 a period of 12 months commencing on the Start Date; 14.9.2 thereafter a period of 12 months commencing on each anniversary of the Start Date; (a) with the final Contract Year ending on the expiry or termination of the Term;
"CREST Service Provider"	means a company with an information security accreditation of a security operations centre qualification from CREST International;
"Cyber Essentials"	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Plus"	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Scheme"	means the Cyber Essentials scheme operated by the NCSC;
"Developed System"	means the software or system that the Supplier is required to develop under this Contract;
"End-User Device"	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic devices used in the provision of the Services;
"Expected Behaviours"	means the expected behaviours set out and updated from time to time in the Government Security Classification Policy, currently found at paragraphs 12 to 16 and in the table below paragraph 16 of https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html;
"Government Data"	Means any: .

(a) data, texts, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media;

(b) Personal Data for which the Buyer is a, or the, Data Controller; or

(c) any meta-data relating to categories of data referred to in Paragraphs (a) or (b);

that is:

(d) supplied to the Supplier by or on behalf of the Buyer; or

(e) that the Supplier is required to generate, Process, Handle, store or transmit under this Contract;

"Government Security Classification Policy"	means the policy, as updated from time to time, establishing an administrative system to protect information assets appropriately against prevalent threats, including classification tiers, protective security controls and baseline behaviours, the current version of which is found at https://www.gov.uk/government/publications/government-security-classifications;
"Handle"	means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data;
"IT Health Check"	means the security testing of the Supplier System;
"Malicious Software"	means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations;
"NCSC"	means the National Cyber Security Centre, or any successor body performing the functions of the National Cyber Security Centre;
"NCSC Device Guidance"	means the NCSC's document "Device Security Guidance", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance;

"Privileged User"	means a user with system administration access to the Supplier System, or substantially similar access privileges;
"Prohibition Notice"	means the meaning given to that term by Paragraph 4.4.
"Protective Monitoring System"	has the meaning given to that term by Paragraph 13.1;
"Relevant Conviction"	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences) or any other offences relevant to Services as the Buyer may specify;
"Remote Location"	means [the relevant Supplier Staff's permanent home address authorised by the Supplier or Sub-contractor (as applicable) for Remote Working OR a location other than a Supplier's or a Sub-contractor's Site];
"Remote Working"	means the provision or management of the Services by Supplier Staff from a location other than a Supplier's or a Sub-contractor's Site;
"Remote Working Policy"	the policy prepared and approved under Paragraph 22 under which Supplier Staff are permitted to undertake Remote Working;
"Security Controls"	means the security controls set out and updated from time to time in the Government Security Classification Policy, currently found at Paragraph 12 of https://www.gov.uk/government/publications/government-security-classifications/guidance-15-considerations-for-security-advisors-html;
"Sites"	means any premises (including the Buyer's Premises, the Supplier's premises or third party premises): (a) from, to or at which: (i) the Services are (or are to be) provided; or (ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or (b) where:

(i) any part of the Supplier System is situated; or

(ii) any physical interface with the Buyer System takes place;

"Staff Vetting Procedure" means the procedure for vetting Supplier Staff set out in Paragraph 6;

"Subcontractor Staff" means:

(a) any individual engaged, directly or indirectly, or employed, by any Subcontractor; and

(b) engaged in or likely to be engaged in:

(i) the performance or management of the Services; or

(ii) the provision of facilities or services that are necessary for the provision of the Services;

Supplier System" means

(a) any:

(i) information assets,

(ii) IT systems,

(iii) IT services; or

(iv) Sites,

that the Supplier or any Subcontractor will use to Handle, or support the Handling of, Government Data and provide, or support the provision of, the Services; and

(b) the associated information management system, including all relevant:

(i) organisational structure diagrams;

(ii) controls;

(iii) policies;

(iv) practices;

(v) procedures;

(vi) processes; and

(vii) resources;

“Third-party Tool” means any software used by the Supplier by which the Government Data is accessed, analysed or modified, or some form of operation is performed on it;

"UKAS-recognised Certification Body" means:

(a) an organisation accredited by UKAS to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022; or

(b) an organisation accredited to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022 by a body with the equivalent functions as UKAS in a state with which the UK has a mutual recognition agreement recognising the technical equivalence of accredited conformity assessment.

PART ONE: CORE REQUIREMENTS

3 HANDLING GOVERNMENT DATA

3.1 The Supplier acknowledges that it:

(a) must only Handle Government Data that is classified as OFFICIAL; and

(b) must not Handle Government Data that is classified as SECRET or TOP SECRET.

3.2 The Supplier must:

(a) not alter the classification of any Government Data.

(b) if it becomes aware that it has Handled any Government Data classified as SECRET or TOP SECRET the Supplier must:

i. immediately inform the Buyer; and

ii. follow any instructions from the Buyer concerning the Government Data.

3.3 The Supplier must, and must ensure that Sub-contractors and Supplier Staff, when Handling Government Data, comply with:

(a) the Expected Behaviours; and

(b) the Security Controls.

4 CERTIFICATION REQUIREMENTS

4.1 Where the Buyer has not specified Certifications under Paragraph 1, the Supplier must ensure that it and any Subcontractors that Handle Government Data are certified as compliant with Cyber Essentials (or equivalent).

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

(a) it; and

(b) any Subcontractor that Processes Government Data,

are certified as compliant with the Certifications specified by the Buyer in Paragraph 1 (or equivalent certifications):

4.3 The Supplier must ensure that the specified Certifications (or their equivalent) are in place for it and any relevant Subcontractor:

(a) before the Supplier or any Subcontractor Handles Government Data; and

(b) throughout the Term.

5 LOCATION

5.1 Where the Buyer has not specified any locations or territories in Paragraph 1, the Supplier must not, and ensure that Subcontractors do not store, access or Handle Government Data outside:

(a) the United Kingdom; or

(b) a location permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).

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

5.3 The Supplier must, and must ensure that its Subcontractors store, access or Handle Government Data in a facility operated by an entity where:

(a) the entity has entered into a binding agreement with the Supplier or Subcontractor (as applicable);(b) that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Subcontractors in this Annex;

(c) the Supplier or Subcontractor has taken reasonable steps to assure itself that:

(i) the entity complies with the binding agreement; and

(ii) the Subcontractor's system has in place appropriate technical and organisational measures to ensure that the Subcontractor will store, access, manage and/or Process the Government Data as required by this Annex;

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

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

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

6 STAFF VETTING

6.1 The Supplier must not allow Supplier Staff, and must ensure that Subcontractors do not allow Subcontractor Staff, to access or Handle Government Data, if that person:

(a) has not completed the Staff Vetting Procedure; or

(b) where no Staff Vetting Procedure is specified in the Order Form:

i. has not undergone the checks required for the BPSS to verify:

A. the individual's identity;

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

C. the individual's previous employment history; and

D. that the individual has no Relevant Convictions; and

ii. national security vetting clearance to the level specified by the Authority for such individuals or such roles as the Authority may specify.

6.2 Where the Supplier considers it cannot ensure that a Sub-contractor will undertake the relevant security checks on any Sub-contractor Staff, it must:

(a) as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;

(b) provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Sub-contractor staff will perform as the Buyer reasonably requires; and

(c) comply, at the Supplier's cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Staff and the management of the Sub-contract.

7 Supplier assurance letter

7.1 The Supplier must, no later than the last day of each Contract Year, provide to the Buyer a letter from its [chief technology officer] (or equivalent officer) confirming that, having made due and careful enquiry:

(a) the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters required by this Contract;

(b) it has fully complied with all requirements of this Annex; and

(c) all Subcontractors have complied with the requirements of this Annex with which the Supplier is required to ensure they comply;

(d) the Supplier considers that its security and risk mitigation procedures remain effective.

8 Assurance

8.1 The Supplier must provide such information and documents as the Buyer may request in order to demonstrate the Supplier's and any Subcontractors' compliance with this Annex.

8.2 The Supplier must provide that information and those documents:

(a) at no cost to the Buyer;

(b) within 10 Working Days of a request by the Buyer;

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

(b) in the case of original document, as a full, unedited and unredacted copy.

9 Use of Subcontractors and third parties

9.1 The Supplier must ensure that Subcontractors and any other third parties that store, have access to or Handle Government Data comply with the requirements of this Annex.

PART TWO: ADDITIONAL REQUIREMENTS

10 SECURITY MANAGEMENT PLAN

10.1 This Paragraph 10 applies only where the Buyer has selected this option in Paragraph 1.3.

Preparation of Security Management Plan

10.2 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Annex and the Contract in order to ensure the security of the Supplier solution and the Buyer data.

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

Approval of Security Management Plan

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

(a) an information security approval statement, which shall confirm that the Supplier may operate the service and process Buyer data; or

(b) a rejection notice, which shall set out the Buyer's reasons for rejection the Security Management Plan.

10.5 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within 10 Working Days of the date of the rejection, or such other period agreed with the Buyer.

10.6 The process set out in Paragraph 10.5 shall be repeated until such time as the Authority issues a Risk Management Approval Statement to the Supplier or terminates this Contract.

10.7 The rejection by the Buyer of a second revised Security Management Plan is a material Default of this Contract.

Updating Security Management Plan

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

Monitoring

10.9 The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:

(a) a significant change to the components or architecture of the Supplier System;

(b) a new risk to the components or architecture of the Supplier System;

(c) a vulnerability to the components or architecture of the Supplier System using an industry standard vulnerability scoring mechanism;

(d) a change in the threat profile;

(e) a significant change to any risk component;

(f) a significant change in the quantity of Personal Data held within the Service;

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

(h) an ISO27001 audit report produced in connection with the Certification indicates significant concerns.

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

11 BUYER SECURITY POLICIES

11.1 The Supplier must comply, when it provides the Services and operates and manages the Supplier System, with all Buyer Security Policies identified in the relevant option in Paragraph 1.3.

11.2 If there is an inconsistency between the Buyer Security Policies and the requirement of this Annex, then the requirements of this Annex will prevail to the extent of that inconsistency.

12 SECURITY TESTING

12.1 The Supplier must:

(a) before Handling Government Data;

(b) at least once during each Contract Year; and

undertake the following activities:

(c) conduct security testing of the Supplier System (an "**IT Health Check**") in accordance with Paragraph 12.2; and

(d) implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph 12.3.

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

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

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

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

(d) ensure that the IT Health Check provides for effective penetration testing of the Supplier System.

12.3 The Supplier treat any vulnerabilities as follows:

(a) the Supplier must remedy any vulnerabilities classified as high in the IT Health Check report:

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

ii. if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3(a)(i) , then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

(b) the Supplier must remedy any vulnerabilities classified as high in the IT Health Check report:

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

ii. if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3(b)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

(c) the Supplier must remedy any vulnerabilities classified as medium in the IT Heath Check report:

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

iv. if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3(c)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

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

2 CLOUD SECURITY PRINCIPLES

2.1 The Supplier must ensure that the Supplier System complies with the Cloud Security Principles.

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

2.2.1 before Handling Government Data;

2.2.2 at least once each Contract Year; and

2.2.3 when required by the Buyer.

2.3 Where the Cloud Security Principles provide for various options, the Supplier must document the option it has chosen to implement and its reasons for doing do.

2.4 The Supplier must:

(a) keep records of any assessment that it makes under Paragraph 13.2; and

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

3 INFORMATION ABOUT SUBCONTRACTORS, SITESAND THIRD-PARTY TOOLS

3.1 The Supplier must keep the following records:

(a) for Subcontractors or third parties that store, have access to or Handle Government Data:

i. the Subcontractor or third party's name:

A. legal name;

B. trading name (if any); and

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

(A) country of registration;

(B) registration number (if applicable); and

(C) registered address;

D. the Certifications held by the Subcontractor or third party;

E. the Sites used by the Subcontractor or third party;

F. the Services provided or activities undertaken by the Subcontractor or third party;

G. the access the Subcontractor or third party has to the Supplier System;

H. the Government Data Handled by the Subcontractor or third party; and

I. the measures the Subcontractor or third party has in place to comply with the requirements of this Annex;

ii. for Sites from or at which Government Data is accessed or Handled:

A. the location of the Site;

B. the operator of the Site, including the operator's:

(A) legal name;

(B) trading name (if any); and

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

C. the Certifications that apply to the Site;

D. the Government Data stored at, or Handled from, the site; and

iii. for Third-party Tools:

A. the name of the Third-Party Tool;

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

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

(A) full legal name;

(B) trading name (if any)

(C) country of registration;

(D) registration number (if applicable); and

(E) registered address.

3.2 The Supplier must update the records it keeps in accordance with Paragraph 14.1:

(a) at least four times each Contract Year;

(b) whenever a Subcontractor, third party that accesses or Handles Government Data, Third-party Tool or Site changes; or

(c) whenever required to go so by the Buyer.

3.3 The Supplier must provide copies of the records it keeps in accordance with Paragraph 14.1 to the Buyer within 10 Working Days of any request by the Buyer.

4 Encryption

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

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

4.1.2 when transmitted.

5 Protective monitoring system

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

(a) identify and prevent any potential Breach of Security;

(b) respond effectively and in a timely manner to any Breach of Security that does;

(c) identify and implement changes to the Supplier System to prevent future any Breach of Security; and

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

(the "**Protective Monitoring System**").

5.2 The Protective Monitoring System must provide for:

(a) event logs and audit records of access to the Supplier System; and

(b) regular reports and alerts to identify:

i. changing access trends;

ii. unusual usage patterns; or

iii. the access of greater than usual volumes of Government Data; and

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

6 PATCHING

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

(a) the Supplier must patch any vulnerabilities classified as "**critical**":

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

ii. if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 17.1(a)(i), then as soon as reasonably practicable after the public release;

(b) the Supplier must patch any vulnerabilities classified as "**important**":

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

ii. if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 17.1(b)(i), then as soon as reasonably practicable after the public release;

(c) the Supplier must remedy any vulnerabilities classified as "**other**" in the public release:

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

ii. if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 17.1(c)(i), then as soon as reasonably practicable after the public release;

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

2 MALWARE PROTECTION

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

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

(a) prevents the installation of the most common forms of Malicious Software in the Supplier System;

(b) performs regular scans of the Supplier System to check for Malicious Software; and

(c) where Malicious Software has been introduced into the Supplier System, so far as practicable

i. prevents the harmful effects from the Malicious Software; and

ii. removes the Malicious Software from the Supplier System.

3 END-USER DEVICES

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

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

(b) users must authenticate before gaining access;

(c) all Government Data must be encrypted using a suitable encryption tool;

(d) the End-User Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-User Device is inactive;

(e) the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Government Data to ensure the security of that Government Data;

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

(g) all End-User Devices are within the scope of any required Certification.

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

4 Vulnerability scanning

4.1 The Supplier must:

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

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

5 Access control

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

(a) identify and authenticate all persons who access the Supplier System before they do so;

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

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

(d) maintain records detailing each person's access to the Supplier System.

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

(a) are allocated to a single, individual user;

(b) are accessible only from dedicated End-User Devices;

(c) are configured so that those accounts can only be used for system administration tasks;

(d) require passwords with high complexity that are changed regularly;

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

(f) are:

i. restricted to a single role or small number of roles;

ii. time limited; and

iii. restrict the Privileged User's access to the internet.

6 REMOTE WORKING

6.1 The Supplier must ensure, and ensure that Sub-contractors ensure, that:

(a) unless in writing by the Authority, Privileged Users do not undertake Remote Working;

(b) where the Authority permits Remote Working by Privileged Users, the Supplier ensures, and ensures that Sub-contractors ensure, that such Remote Working takes place only in accordance with any conditions imposed by the Authority.

6.2 Where the Supplier or a Sub-contractor wishes to permit Supplier Staff to undertake Remote Working, it must:

(a) prepare and have approved by the Buyer in the Remote Working Policy in accordance with this Paragraph;

(b) undertake and, where applicable, ensure that any relevant Sub-contractors undertake, all steps required by the Remote Working Policy;

(c) ensure that Supplier Staff undertake Remote Working only in accordance with the Remote Working Policy;

(d) may not permit any Supplier Staff or the Supplier or any Sub-contractor to undertake Remote Working until the Remote Working Policy is approved by the Buyer.

6.3 The Remote Working Policy must include or make provision for the following matters:

(a) restricting or prohibiting Supplier Staff from printing documents in any Remote Location;

(b) restricting or prohibiting Supplier Staff from downloading any Government Data to any End-User Device other than an End User Device that:

i. is provided by the Supplier or Sub-contractor (as appropriate); and

ii. complies with the requirements set out in Paragraph 3 (*End-User Devices*);

(c) ensuring that Supplier Staff comply with the Expected Behaviours (so far as they are applicable);

(d) giving effect to the Security Controls (so far as they are applicable); and

(e) for each different category of Supplier Staff subject to the proposed Remote Working Policy:

i. the types and volumes of Government Data that the Supplier Staff can Handle in a Remote Location and the Handling that those Supplier Staff will undertake;

ii. any identified security risks arising from the proposed Handling in a Remote Location;

iii. the mitigations, controls and security measures the Supplier or Sub-contractor (as applicable) will implement to mitigate the identified risks; and

iv. the business rules with which the Supplier Staff must comply.

6.4 The Supplier may submit a proposed Remote Working Policy for consideration at any time.

7 BACKUP AND RECOVERY OF GOVERNMENT DATA

7.1 The Supplier must ensure that the Supplier System:

(a) backs up and allows for the recovery of Government Data to achieve the recovery point and recovery time objectives specified by the Buyer, or in accordance with Good Industry Practice where the Buyer has not specified; and

(b) retains backups of the Government Data for the period specified by the Buyer, or in accordance with Good Industry Practice where the Buyer has not specified.

7.2 The Supplier must ensure the Supplier System:

(a) uses backup location for Government Data that are physically and logically separate from the rest of the Supplier System;

(b) the backup system monitors backups of Government Data to:

i. identify any backup failure; and

ii. confirm the integrity of the Government Data backed up;

(c) any backup failure is remedied properly;

(d) the backup system monitors backups of Government Data to:

i. identify any recovery failure; and

ii. confirm the integrity of Government Data recovered; and

(e) any recovery failure is promptly remedied.

8 Return and deletion of Government Data

8.1 Subject to Paragraph 24.2, when requested to do so by the Buyer, the Supplier must, and must ensure that all Subcontractors:

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

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

24.2 Paragraph 24.1 does not apply to Government Data:

(a) that is Personal Data in respect of which the Supplier is a Controller;

(b) to which the Supplier has rights to Handle independently from this Contract; or

(c) in respect of which, the Supplier is under an obligation imposed by Law to retain.

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

(a) when requested to do so by the Buyer; and

(b) using the method specified by the Buyer.

25 PHYSICAL SECURITY

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

26 BREACH OF SECURITY

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

(a) notify the Buyer as soon as reasonably practicable after becoming aware of the breach, and in any event within [24] hours;

(b) provide such assistance to the Buyer as the Buyer requires until the Breach of Security and any impacts or potential impacts on the Buyer are resolved to the Buyer's satisfaction;

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