

G-Cloud 14 Call-Off Contract

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

G-Cloud 14 Call-Off Contract

Part A: Order Form	2
Part B: Terms and conditions	12
Schedule 1: Services	33
Schedule 2: Call-Off Contract charges	34
Schedule 3: Collaboration agreement	35
Schedule 4: Alternative clause	48
Schedule 5: Guarantee	52
Schedule 6: Glossary and interpretations	60
Schedule 7: UK GDPR Information	76
Annex 1: Processing Personal Data	76
Annex 2: Joint Controller Agreement	80
Schedule 8: Corporate Resolution Planning	88
Schedule 9 : Variation Form	110

Part A: Order Form

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

Platform service ID number	230924019529259
Call-Off Contract reference	QUO-241210-23163 PROC-922-2024
Call-Off Contract title	TOPdesk Cloud Software
Call-Off Contract description	TOPdesk Cloud Software
Start date	1 st March 2025
Expiry date	28 th February 2026
Call-Off Contract value	£ 46,426.36 (ex-VAT) per Annum plus [REDACTED] ex-VAT) Consultancy Fee
Charging method	Submission of Supplier Invoice
Purchase order number	TBC

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	<p>Competition & Markets Authority</p> <p>██████████</p> <p>██████████████████</p> <p>██████████</p> <p>██████████</p>
To the Supplier	<p>TOPdesk UK Limited</p> <p>Tel: ██████████ Supplier's Address:</p> <p>██████████████████████████████</p> <p>██████████████████</p> <p>██████████████</p> <p>██████████████</p> <p>██████████</p> <p>██████████████████</p> <p>██</p>
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: [REDACTED]
Name: [REDACTED]
[REDACTED]
Phone: [REDACTED]

For the Supplier:

Title: [REDACTED]
Name: [REDACTED]
[REDACTED]
Phone: [REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 1st March 2025 and is valid until 28 th February 2026.
Ending (termination)	<p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums (as per clause 18.6).</p> <p>The notice period for the Buyer is a maximum of 30 days from the date of written notice for Ending without cause (as per clause 18.1).</p>

Extension period	<p>This Call-Off Contract can be extended by the Buyer for 1 period of up to 12 months, by giving the 90 calendar days written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.</p> <p>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.</p>
-------------------------	--

Buyer contractual details

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

G-Cloud Lot	<p>This Call-Off Contract is for the provision of Services Under:</p> <ul style="list-style-type: none"> • Lot 2: Cloud software
G-Cloud Services required	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below: https://www.topdesk.com/en/pricing/</p> <p>Provision of a Service Management solution.</p> <ul style="list-style-type: none"> • ITIL Aligned • Customer-driven, continuously deployed release cycle

	<ul style="list-style-type: none"> • Intuitive, contemporary and highly configurable Self-Service portal • Powerful API complimented by inbuilt scripting tools for easy integrations • Kanban board for Agile working • Code-free designers for processes and Self-Service Portal • Simple links with AD using Azure • Inbuilt Events and Actions tool for creating automated alerts / notifications • Scalable mobile solution for on-the-go use • In-tool reporting wizard with OData feed • Integration with Microsoft Endpoint Manager <p>TOPdesk Excellent package includes:</p> <ul style="list-style-type: none"> • Incident Management • Asset Management • Self-Service Portal • Knowledge base • Dashboard & reporting • 1 sandbox environment • Unlimited assets • Unlimited email, AD and SSO integrations • Change Management • Problem Management • Contract & SLM • Operations management • Survey Management • Webshop • Project Management • TOPdesk Feedback Solution • TOPdesk Asset Audit
Additional Services	Not Applicable
Location	<p>The Services will be delivered to:</p> <p>Competition & Markets Authority</p>

	<p>██████████</p> <p>██████████████████</p> <p>██████████</p> <p>██████████</p>
Quality Standards	<p>The quality standards required for this Call-Off Contract are as per the G-Cloud framework standards in clause 14. TOPdesk is SOC 2 certified. All of the data centres used to host the service are ISO 27001 accredited.</p>
Technical Standards:	<p>The technical standards used as a requirement for this Call-Off Contract are</p> <ul style="list-style-type: none"> - SOC2 - ITIL
Service level agreement:	<p>The service level and availability criteria required for this Call-Off Contract are detailed in the Supplier's Service Level Agreement 2024 (Attached)</p> <p>TOPdesk brochure EN</p>
Onboarding	<p>The onboarding plan for this Call-Off Contract is as detailed in the Supplier's Service Definition document and includes (2) day's implementation and training. All costs are included in the contract.</p>

Offboarding	<p>The offboarding plan for this Call-Off Contract detailed in the Supplier's Service Definition document.</p> <p>https://page.topdesk.com/saas-information#exitstrategy</p>
--------------------	---

	At the end of a contract, customers can extract their data at no extra cost.
Collaboration agreement	Not Applicable
Limit on Parties' liability	<p>Defaults by either party resulting in direct loss or damage to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed £ 46,426.36 per year. The cap on any property-related claims will be (12) twelve calendar months' worth of the Fees.</p> <p>The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation of or damage to any Buyer Data will not exceed £46,426.36 or] (12) twelve calendar months' worth of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>The annual total liability of the Supplier for all other Defaults will not exceed the greater of £46,426.36 or (12) twelve calendar months' worth of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>
Buyer's responsibilities	The Buyer is responsible for allowing the Supplier's relevant personnel and approved subcontractors access to the required systems and sites as relevant to complete the schedule of services and outcomes in this Agreement.

Buyer's equipment	No equipment required
--------------------------	-----------------------

Supplier's information

Subcontractors or partners	Not Applicable
-----------------------------------	----------------

Call-Off Contract charges and payment

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

Payment method	The payment method for this Call-Off Contract is BACS
Payment profile	The payment profile for this Call-Off Contract is as set out in Schedule 2: Call Off Contract Charges.
Invoice details	The Supplier will issue electronic invoices at the frequency set out in the Schedule 2: Call Off Contract Charges. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.

Who and where to send invoices to	Invoices will be sent to Efe Amgbah ([REDACTED])
Invoice information required	All invoices must include purchase order reference.
Invoice frequency	Invoice will be sent to the Buyer annually in advance.
Call-Off Contract value	The total value of this Call-Off Contract is £48,266.36 (ex-VAT).
Call-Off Contract charges	The breakdown of the Charges is shown in Schedule 2: Call Off Contract Charges.

Additional Buyer terms

Performance of the Service	<p>This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones:</p> <ul style="list-style-type: none">• As detailed in the Supplier's Service Level Agreement 2024 document.
Guarantee	Not Applicable
Warranties, representations	<p>In addition to the incorporated Framework Agreement clause 2.3, the Supplier warrants and represents to the Buyer that its Personnel and its sub-contractors take all reasonable precautions at no additional cost to the Buyer to ensure that no known Viruses are coded or introduced into the Licensed Programs.</p>

	<p>The Supplier warrants that during the Term:</p> <ol style="list-style-type: none"> 1. It will attain the standards of reasonable care and skill commensurate with those currently prevailing in the software industry in fulfilling its obligations under this Agreement; 2. all of its personnel have qualifications and experience appropriate for the tasks to which they are allocated; 3. it has full capacity and authority and all necessary licences, permits, permissions, powers and consents to enter into and to perform this Agreement; 4. it has a valid licence to the Intellectual Property Rights in the licensed programs; and 5. it has and shall maintain an appropriate disaster recovery and business continuity plan. <p>When serving the Supplier written notification of a defect in the licensed programs, the Buyer shall provide to the Supplier all information reasonably required by the Supplier to correct the defect and a documented example of the defect. Upon the Supplier's receipt of such information and documented example, the Supplier shall, at no additional cost to the Buyer, use its best endeavours to correct the defect in a reasonable time period and provide written notification to the Buyer as to the correction of the defect. The Supplier shall be permitted to install temporary solutions, program bypasses and/or problem avoiding limitations in the licensed programs to correct the defect. If the Supplier does not correct the defect in a reasonable time period, the Buyer shall be entitled to forthwith terminate this Agreement by written notice to the Supplier.</p> <p>Exceptions:</p> <p>The supplier's warranties above shall not apply if the defect is non-reproducible and/or arises out of or is exacerbated by:</p> <p>any incorrect use, operation or corruption of the licensed programs;</p> <p>any unauthorised development, modification, enhancement, alteration or change of the licensed programs; and/or</p> <p>use of the licensed program materials with any software, equipment or programs not supplied or approved by the Supplier.</p> <p>If a defect is non-reproducible or arises from the exclusions noted above, the Supplier reserves the right to charge the Buyer for any corrective actions needed at its prevailing rates. In such cases, the Supplier shall not be deemed in breach of its obligations under this Agreement.</p>
--	--

	<ul style="list-style-type: none"> - The Supplier neither warrants that the Licensed Programs are free of any minor defects, errors or Bugs nor that the Licensed Programs operate free of any disruption, outages or breakdowns nor that the Supplier will review the Buyer's data for accuracy nor that the licensed programs are fit for purpose or otherwise meet the Buyer's expectations. - The Supplier does not provide any warranty in relation to and disclaims all liability and responsibility for any third party products or services not provided by the Supplier and for the acts or omissions of any provider of such third party products or services. - The Supplier does not guarantee that our security procedures will be error-free or that transmissions of the Buyer's data will always be secure or that unauthorised third parties will never be able to defeat the Supplier's security measures or those of its sub-contractors. - The Supplier does not guarantee the accuracy and completeness of the information provided or supplied by the Supplier through whatever medium, including the Supplier's website, portals, email and orally by or on behalf of the Supplier directly or indirectly to the Buyer.
Supplemental requirements in addition to the Call-Off terms	The Buyer includes the entirety of Annex 4 as Supplementary Requirements in addition to the Call-Off terms.
Alternative clauses	Not Applicable

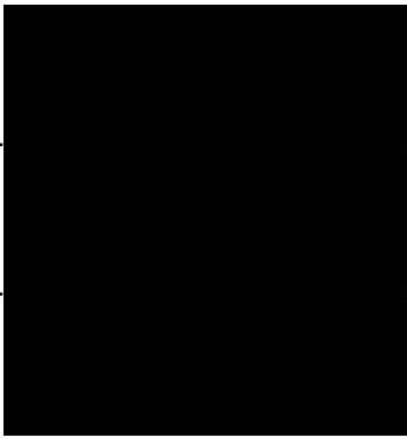
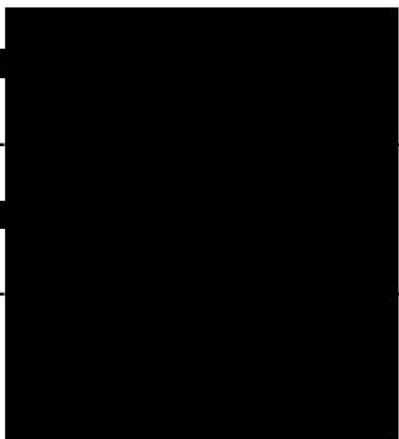
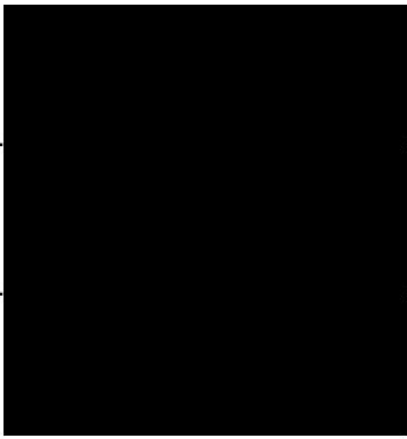
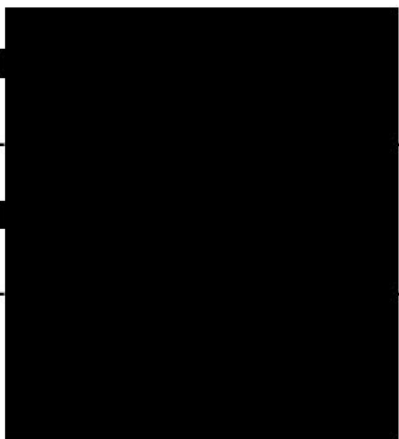
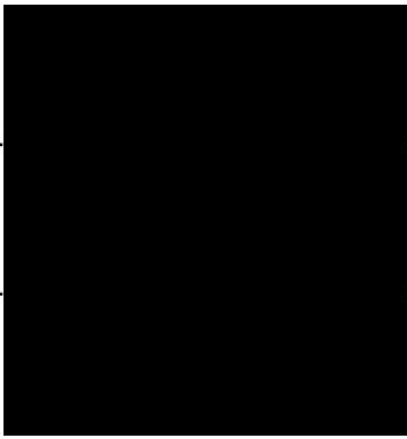
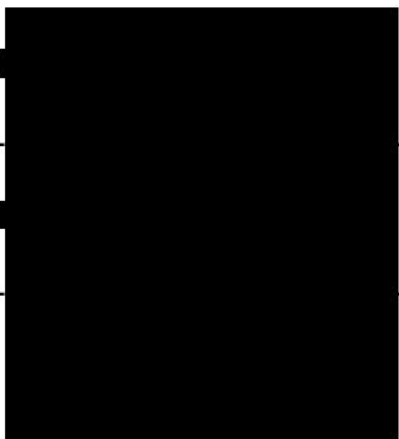
Buyer specific amendments to/refinements of the Call-Off Contract terms	Not Applicable
Personal Data and Data Subjects	Annex 1 of Schedule 7 is being used: https://page.topdesk.com/gdpr
Intellectual Property	Not Applicable
Social Value	Not Applicable
Performance Indicators	Data supplied by the Supplier in relation to Performance Indicators is deemed the Intellectual Property of the Buyer and may be published by the Buyer.

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		
Title		
Signature		
Date	30 January 2025 10:56 CET	20/01/2025

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

Buyer Benefits

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

[G-Cloud 14 Buyer 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

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

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

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

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

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

3. Supply of services

- 3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.
- 3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

4. Supplier staff

4.1 The Supplier Staff must:

- 4.1.1 be appropriately experienced, qualified and trained to supply the Services
- 4.1.2 apply all due skill, care and diligence in faithfully performing those duties

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

5. Due diligence

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

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

6. Business continuity and disaster recovery

- 6.1 The Supplier will have a clear business continuity and disaster recovery plan in their Service Descriptions.
- 6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.
- 6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

- 7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.
- 7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
- 7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.
- 7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.
- 7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.
- 7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.
- 7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.
- 7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
- 7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.
- 7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay

undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.
- 7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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

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

9. Insurance

- 9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.
- 9.2 The Supplier will ensure that:
 - 9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
 - 9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit
 - 9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
 - 9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

- 9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.
- 9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:
 - 9.4.1 a broker's verification of insurance
 - 9.4.2 receipts for the insurance premium
 - 9.4.3 evidence of payment of the latest premiums due
- 9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:
 - 9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
 - 9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances
 - 9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

10. Confidentiality

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

11. Intellectual Property Rights

- 11.1 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.
- 11.2 Neither Party shall have any right to use any of the other Party's names, logos or trademarks on any of its products or services without the other Party's prior written consent.
- 11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:

- 11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and
- 11.3.2 The Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer's written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.
- 11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.
- 11.5 Subject to the limitation in Clause 24.3, the Buyer shall:
- 11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:
- (a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
 - (b) alleging that the Buyer Data violates, infringes or misappropriate any rights of a third party;
 - (c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and
- 11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgement against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer's obligations under this Clause 11.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier's breach of this Contract.
- 11.6 The Supplier will, on written demand, fully indemnify the Buyer for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:
- 11.6.1 rights granted to the Buyer under this Call-Off Contract
- 11.6.2 Supplier's performance of the Services
- 11.6.3 use by the Buyer of the Services
- 11.7 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:
- 11.7.1 modify the relevant part of the Services without reducing its functionality or performance

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

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

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

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

11.8.2 other material provided by the Buyer necessary for the Services

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

12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

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

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

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

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

13. Buyer data

- 13.1 The Supplier must not remove any proprietary notices in the Buyer Data.
- 13.2 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.
- 13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.
- 13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.
- 13.5 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.
- 13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

13.6.1 the principles in the Security Policy Framework:

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

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

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

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

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance:

<https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>

13.6.6 Buyer requirements in respect of AI ethical standards.

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

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

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

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

14. Standards and quality

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

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

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

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

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

15. Open source

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

16. Security

- 16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.
- 16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
- 16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.
- 16.4 Responsibility for costs will be at the:
 - 16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided
 - 16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control
- 16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.
- 16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:
<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>

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

17. Guarantee

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

17.1.1 an executed Guarantee in the form at Schedule 5

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

18. Ending the Call-Off Contract

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

- 18.2 The Parties agree that the:

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

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

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

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

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

18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)

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

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

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

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

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

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

19.5.4 destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law

19.5.5 work with the Buyer on any ongoing work

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

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

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

20. Notices

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

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

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

21. Exit plan

- 21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.
- 21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.
- 21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.
- 21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.
- 21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.
- 21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from CDDO under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:
- 21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the period on terms that are commercially reasonable and acceptable to the Buyer
- 21.6.2 there will be no adverse impact on service continuity

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

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

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

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

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

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

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

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

22. Handover to replacement supplier

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

23. Force majeure

- 23.1 Neither Party will be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Call-Off Contract (other than a payment of money) to the extent that such delay or failure is a result of a Force Majeure event.
- 23.2 A Party will promptly (on becoming aware of the same) notify the other Party of a Force Majeure event or potential Force Majeure event which could affect its ability to perform its obligations under this Call-Off Contract.
- 23.3 Each Party will use all reasonable endeavours to continue to perform its obligations under the Call-Off Contract and to mitigate the effects of Force Majeure. If a Force Majeure event prevents a Party from performing its obligations under the Call-Off Contract for more than 30 consecutive Working Days, the other Party can End the Call-Off Contract with immediate effect by notice in writing.

24. Liability

- 24.1 Subject to incorporated Framework Agreement clauses 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).
- 24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Supplier's liability:
- 24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited; and
- 24.2.2 in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.
- 24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).
- 24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause 24.2 will not be taken into consideration.

25. Premises

- 25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.
- 25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.
- 25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.
- 25.4 This clause does not create a tenancy or exclusive right of occupation.
- 25.5 While on the Buyer's premises, the Supplier will:
 - 25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises
 - 25.5.2 comply with Buyer requirements for the conduct of personnel
 - 25.5.3 comply with any health and safety measures implemented by the Buyer
 - 25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury
- 25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

- 26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.
- 26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.
- 26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

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

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

28. Environmental requirements

- 28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.
- 28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

- 29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.
- 29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to end it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:
- 29.2.1 the activities they perform
 - 29.2.2 age
 - 29.2.3 start date
 - 29.2.4 place of work
 - 29.2.5 notice period
 - 29.2.6 redundancy payment entitlement
 - 29.2.7 salary, benefits and pension entitlements
 - 29.2.8 employment status
 - 29.2.9 identity of employer
 - 29.2.10 working arrangements
 - 29.2.11 outstanding liabilities
 - 29.2.12 sickness absence
 - 29.2.13 copies of all relevant employment contracts and related documents
 - 29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer.

- 29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.
- 29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.
- 29.5 The Supplier will cooperate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.
- 29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:
- 29.6.1 its failure to comply with the provisions of this clause
 - 29.6.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer
- 29.7 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.
- 29.8 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

The TOPdesk offering always comes with the same powerful, easy-to-use platform that includes unlimited assets, local support by real people, AD integration(s), full access to APIs, mobile access/capabilities, an extensive knowledge base, reporting and dashboarding capabilities and the ability to register information about your personnel and organisation.

2.1 Overview of TOPdesk Packages

TOPdesk designed three plans to fit your organisation's needs: Essential, Engaged and Excellent. Below you'll find a detailed description of these plans and what they contain.



Manage your assets, offer a self-service portal and solve customer requests.

TOPdesk platform, plus:

- Incident Management
- Asset Management
- Self-Service Portal
- Knowledge Base
- Dashboards & Reporting
- One Sandbox environment
- Unlimited assets
- Unlimited e-mail, AD and SSO integrations



All the features you need to manage complex workflows.

Everything in Essential, plus:

- Change Management
- Problem Management
- Contract & Service Level Management
- Operations Management
- Survey Management



Complete service plan for the best customer experience.

Everything in Engaged, plus:

- Project Management
- Stock & Order Management
- 24/5 support*
- Annual health check

* As per TOPdesk's Service Level Agreement

Schedule 2: Call-Off Contract charges

3. Your TOPdesk solution

The overview below lists the monthly investment for the TOPdesk solution.

TOPdesk Excellent	
Number of licensed agents	Price per month
System integration	
Total Price per Year TOPdesk Excellent	

The rates listed in the overview are valid from 01-10-2024. TOPdesk reserves the right to adjust the rates without prior notice. The costs listed above are excluding VAT and implementation costs.

4. TOPdesk implementation services

The overview below lists the elements of the TOPdesk implementation as discussed with you during the lead-up to this proposal.

TOPdesk consultancy

The rates listed in the overview are valid from 01-10-2024. TOPdesk reserves the right to adjust the rates without prior notice. These rates do not include VAT.

Consultancy services

It has been agreed that the consultancy/training above will be delivered **remotely**.

Prices mentioned do not include VAT.

Rates are based on consultancy days lasting from 10 a.m. to 5 p.m. (GMT/BST) with the customer and include a one-hour lunch. The final costs are determined by recalculation and will be invoiced per individual day. You are not billed for unused consultancy days. You can request an additional quotation from TOPdesk for extra consultancy days.

Schedule 3: Collaboration agreement- Not Applicable

1.

Schedule 4: Alternative clauses- Not Applicable

1.

Schedule 5: Guarantee- Not Applicable

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

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

Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form, set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, Personal Data and any information, which may include (but isn't limited to) any: <ul style="list-style-type: none"> • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the UK GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.

Data Protection Legislation (DPL)	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
Data Subject	Takes the meaning given in the UK GDPR
Default	<p>Default is any:</p> <ul style="list-style-type: none"> • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract <p>Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.</p>
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	<p>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:</p> <p>https://www.gov.uk/guidance/check-employment-status-fortax</p>
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Financial Metrics	<p>The following financial and accounting measures:</p> <ul style="list-style-type: none"> • Dun and Bradstreet score of 50 • Operating Profit Margin of 2% • Net Worth of 0 • Quick Ratio of 0.7

Force Majeure	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.14 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).

Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	Can be: <ul style="list-style-type: none"> • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium • a Supplier Trigger Event
Intellectual Property Rights or IPR	Intellectual Property Rights are: <p>(a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information</p> <p>(b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction</p> <ul style="list-style-type: none"> • (c) all other rights having equivalent or similar effect in any country or jurisdiction

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

Know-How	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	<p>To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:</p> <ul style="list-style-type: none"> • induce that person to perform improperly a relevant function or activity • reward that person for improper performance of a relevant function or activity • commit any offence: <ul style="list-style-type: none"> ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.

Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service Data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data and Performance Indicators data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls <u>ck-if-you-need-approval-to-spend-money-on-a-service</u>

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

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

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

Intentionally Blank

Schedule 7: UK GDPR Information

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

Annex 1 - Processing Personal Data

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

1.1 The contact details of the Buyer's Data Protection Officer are: **Bart van Manen**

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

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

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

Description	Details
Identity of Controller and Processor for each Category of Personal Data	The Buyer is Controller and the Supplier is Processor The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: <ul style="list-style-type: none">• .Personal contact details and details of calls logged.
Duration of the Processing	Contract duration plus 30 days after contract end date.
Nature and purposes of the Processing	The nature and purpose of the processing is to record, categorise and manage the end to end process of customer incidents and requests within the TopDesk software. To manage various other ITIL aligned processes such as problem, change and asset management. The purpose is to record and manage through to completion a variety of IT related processes, to support the organisations IT department and to gather management information from the recorded data
Type of Personal Data	Staff name, office location, office telephone number, organisational role, username, password, line manager

Categories of Data Subject	Staff including permanent employees, contractors, temporary staff, volunteers, also IT assets, office locations, third party providers, IT services, IT analysts.
International transfers and legal gateway	<p>TOPdesk currently offers hosting locations in Australia (AU), Brazil (BR), Canada (CA), the European Union (NL and EU), Norway (NO), the United Kingdom (UK), and the United States of America (US).</p> <p>Customers can choose where their data is stored and can verify this location via our customer service portal (My TOPdesk). Data is never moved to another region without the written confirmation from a SaaS main contact at the customer. Off-site back-ups are stored on a different location within the same region*, ensuring the same conditions apply.</p>
Plan for return and destruction of the data once the Processing is complete	<p>After terminating a contract, we keep data for 30 days and remove it automatically after this period. To ensure that data is completely deleted, we have an automatic system with a built-in control mechanism for the deletion. We also have a monitoring system that actively scans folders, databases and live environments for data that should have been removed. If data has not already been downloaded, customers can contact TOPdesk Support to request a copy. Up to 30 days after terminating a contract, one of a customer's nominated contacts can request your data through our Self-Service Portal. Upon this request, we will send the data as soon as possible through a secure connection. All data comes in a regular file format. Redundant hard discs are destroyed only by an ADISA (Asset Disposal and Information Security Alliance) certified company. Hard discs are destroyed by crushing; CDs/DVDs are shredded. This does not achieve the Disposal of data-bearing media are, for OFFICIAL carried out in accordance with industry and UK Government best practice: Hard disc: break the platters into at least four pieces. Optical media: shred or break to pieces 6mm maximum in any direction UK Government RESTRICTED information contained on any media device is destroyed in accordance with BS EN 15713:2009 standard and destruction certificates issued.</p>

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.

2. Undertakings of both Parties

2.1 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.

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

3. Data Protection Breach

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

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

(b) all reasonable assistance, including:

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

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

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

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

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

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

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

- (d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;
- (e) measures taken or proposed to be taken to address the Personal Data Breach; and
- (f) describe the likely consequences of the Personal Data Breach.

4. Audit

4.1 The Supplier shall permit:

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

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

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

5. Impact Assessments

5.1 The Parties shall:

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

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

6. ICO Guidance

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

7. Liabilities for Data Protection Breach

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

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

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

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

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

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

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

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

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

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Buyer and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result

of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Buyer.

8. Termination

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

9. Sub-Processing

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

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

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

10. Data Retention

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

Schedule 8 (Corporate Resolution Planning)

1. Definitions

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

"Accounting Reference Date"	means in each year the date to which the Supplier prepares its annual audited financial statements;
"Annual Revenue"	<p>means, for the purposes of determining whether an entity is a Public Sector Dependent Supplier, the audited consolidated aggregate revenue (including share of revenue of joint ventures and Associates) reported by the Supplier or, as appropriate, the Supplier Group in its most recent published accounts, subject to the following methodology:</p> <p>figures for accounting periods of other than 12 months should be scaled pro rata to produce a proforma figure for a 12 month period; and</p> <p>where the Supplier, the Supplier Group and/or their joint ventures and Associates report in a foreign currency, revenue should be converted to British Pound Sterling at the closing exchange rate on the Accounting Reference Date;</p>

“Appropriate Authority” or “Appropriate Authorities”	means the Buyer and the Cabinet Office Markets and Suppliers Team or, where the Supplier is a Strategic Supplier, the Cabinet Office Markets and Suppliers Team;
“Associates”	means, in relation to an entity, an undertaking in which the entity owns, directly or indirectly, between 20% and 50% of the voting rights and exercises a degree of control sufficient for the undertaking to be treated as an associate under generally accepted accounting principles;
"Cabinet Office Markets and Suppliers Team"	means the UK Government’s team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function;
“Class 1 Transaction”	has the meaning set out in the listing rules issued by the UK Listing Authority;
“Control”	the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares,

	by contract or otherwise) and “Controls” and “Controlled” shall be interpreted accordingly;
“Corporate Change Event”	<p>means:</p> <ul style="list-style-type: none"> (a) any change of Control of the Supplier or a Parent Undertaking of the Supplier; (b) any change of Control of any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Services; (c) any change to the business of the Supplier or any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Services; (d) a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the London Stock Exchange plc; (e) an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking place in respect of the Supplier or any Parent Undertaking of the Supplier; (f) payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the Net Asset Value of the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any 12 month period; (g) an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group; (h) any member of the Supplier Group stopping payment of its debts generally or becoming unable to pay its debts within the meaning of section 123(1) of the Insolvency Act 1986 or any member of the Supplier Group ceasing to carry on all or substantially all its business, or any compromise, composition, arrangement or agreement being made with creditors of any member of the Supplier Group; (i) the appointment of a receiver, administrative receiver or administrator in respect of or over all or a material part of the undertaking or assets of any member of the Supplier Group; and/or

	(j) any process or events with an effect analogous to those in paragraphs (e) to (g) inclusive above occurring to a member of the Supplier Group in a jurisdiction outside England and Wales;
"Corporate Change Event Grace Period"	means a grace period agreed to by the Appropriate Authority for providing CRP Information and/or updates to Business Continuity Plan after a Corporate Change Event;
"Corporate Resolvability Assessment (Structural Review)"	means part of the CRP Information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraph 3 and Annex 2 of this Schedule;
"Critical National Infrastructure" or "CNI"	<p>means those critical elements of UK national infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:</p> <p>major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or</p> <p>significant impact on the national security, national defence, or the functioning of the UK;</p>

“Critical Service Contract”	means the overall status of the Services provided under the Call-Off Contract as determined by the Buyer and specified in Paragraph 2 of this Schedule;
“CRP Information”	<p>means the corporate resolution planning information, together, the:</p> <p>(a) Exposure Information (Contracts List);</p> <p>(b) Corporate Resolvability Assessment (Structural Review); and</p> <p>(c) Financial Information and Commentary</p>
“Dependent Parent Undertaking”	means any Parent Undertaking which provides any of its Subsidiary Undertakings and/or Associates, whether directly or indirectly, with any financial, trading, managerial or other assistance of whatever nature, without which the Supplier would be unable to continue the day to day conduct and operation of its business in the same manner as carried on at the time of entering into the Call-Off Contract, including for the avoidance of doubt the provision of the Services in accordance with the terms of the Call-Off Contract;
“FDE Group” “Financial Distress Event”	<p>means the [Supplier, Subcontractors, [the Guarantor]</p> <p>the credit rating of an FDE Group entity dropping below the applicable Financial Metric;</p>

	<p>an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;</p> <p>there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity;</p> <p>an FDE Group entity committing a material breach of covenant to its lenders;</p> <p>a Subcontractor notifying CCS or the Buyer that the Supplier has not satisfied any material sums properly due under a specified invoice and not subject to a genuine dispute;</p> <p>any of the following:</p> <p>commencement of any litigation against an FDE Group entity with respect to financial indebtedness greater than £5m or obligations under a service contract with a total contract value greater than £5m;</p> <p>non-payment by an FDE Group entity of any financial indebtedness;</p> <p>any financial indebtedness of an FDE Group entity becoming due as a result of an event of default;</p> <p>the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity; or</p> <p>the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity;</p> <p>in each case which the Buyer reasonably believes (or would be likely to reasonably believe) could directly impact on the continued performance and delivery of the Services in accordance with the Call-Off Contract; and</p> <p>any two of the Financial Metrics for the Supplier not being met at the same time.</p>
“Parent Undertaking”	<p>has the meaning set out in section 1162 of the Companies Act 2006;</p>

“Public Sector Dependent Supplier”	means a supplier where that supplier, or that supplier’s group has Annual Revenue of £50 million or more of which over 50% is generated from UK Public Sector Business;
“Strategic Supplier”	means those suppliers to government listed at https://www.gov.uk/government/publications/strategic-suppliers ;
“Subsidiary Undertaking”	has the meaning set out in section 1162 of the Companies Act 2006;
“Supplier Group”	means the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings;
“UK Public Sector Business”	means any goods, service or works provision to UK public sector bodies, including Central Government Departments and their arm's length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police, fire and rescue, education bodies and devolved administrations; and

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

2. Service Status and Supplier Status

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

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

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

3. Provision of Corporate Resolution Planning Information

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

3.2 Subject to Paragraphs 3.6, 3.10 and 3.11:

3.2.1 where the Call-Off Contract is a Critical Service Contract, the Supplier shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the Start Date; and

3.2.2 except where it has already been provided, where the Supplier is a Public Sector Dependent Supplier, it shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the date of the Appropriate Authority's or Appropriate Authorities' request.

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

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

3.3.2 is split into three parts:

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

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

- 3.3.3 incorporates any additional commentary, supporting documents and evidence which would reasonably be required by the Appropriate Authority or Appropriate Authorities to understand and consider the information for approval;
 - 3.3.4 provides a clear description and explanation of the Supplier Group members that have agreements for goods, services or works provision in respect of UK Public Sector Business and/or Critical National Infrastructure and the nature of those agreements; and
 - 3.3.5 complies with the requirements set out at Annex 1 (Exposure Information (Contracts List)), Annex 2 (Corporate Resolvability Assessment (Structural Review)) and Annex 3 (Financial Information and Commentary) respectively.
- 3.4 Following receipt by the Appropriate Authority or Appropriate Authorities of the CRP Information pursuant to Paragraphs 3.2, 3.8 and 3.9, the Buyer shall procure that the Appropriate Authority or Appropriate Authorities shall discuss in good faith the contents of the CRP Information with the Supplier and no later than 60 days after the date on which the CRP Information was delivered by the Supplier either provide an Assurance to the Supplier that the Appropriate Authority or Appropriate Authorities approve the CRP Information or that the Appropriate Authority or Appropriate Authorities reject the CRP Information.
- 3.5 If the Appropriate Authority or Appropriate Authorities reject the CRP Information:
- 3.5.1 the Buyer shall (and shall procure that the Cabinet Office Markets and Suppliers Team shall) inform the Supplier in writing of its reasons for its rejection; and
 - 3.5.2 the Supplier shall revise the CRP Information, taking reasonable account of the Appropriate Authority's or Appropriate Authorities' comments, and shall re-submit the CRP Information to the Appropriate Authority or Appropriate Authorities for approval within 30 days of the date of the Appropriate Authority's or Appropriate Authorities' rejection. The provisions of paragraph 3.3 to 3.5 shall apply again to any resubmitted CRP Information provided that either Party

may refer any disputed matters for resolution under clause 32 of the Framework Agreement (Managing disputes).

- 3.6 Where the Supplier or a member of the Supplier Group has already provided CRP Information to a central government body or the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely to the Cabinet Office Markets and Suppliers Team) and has received an Assurance of its CRP Information from that central government body and the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely from the Cabinet Office Markets and Suppliers Team), then provided that the Assurance remains Valid (which has the meaning in paragraph 3.7 below) on the date by which the CRP Information would otherwise be required, the Supplier shall not be required to provide the CRP Information under Paragraph 3.2 if it provides a copy of the Valid Assurance to the Appropriate Authority or Appropriate Authorities on or before the date on which the CRP Information would otherwise have been required.
- 3.7 An Assurance shall be deemed Valid for the purposes of Paragraph 3.6 if:
- 3.7.1 the Assurance is within the validity period stated in the Assurance (or, if no validity period is stated, no more than 12 months has elapsed since it was issued and no more than 18 months has elapsed since the Accounting Reference Date on which the CRP Information was based); and
 - 3.7.2 no Corporate Change Events or Financial Distress Events (or events which would be deemed to be Corporate Change Events or Financial Distress Events if the Call-Off Contract had then been in force) have occurred since the date of issue of the Assurance.
- 3.8 If the Call-Off Contract is a Critical Service Contract, the Supplier shall provide an updated version of the CRP Information (or, in the case of Paragraph 3.8.3 of its initial CRP Information) to the Appropriate Authority or Appropriate Authorities:
- 3.8.1 within 14 days of the occurrence of a Financial Distress Event (along with any additional highly confidential information no longer exempted from disclosure under Paragraph 3.11)

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

3.8.2 within 30 days of a Corporate Change Event unless

- (a) the Supplier requests and the Appropriate Authority (acting reasonably) agrees to a Corporate Change Event Grace Period, in the event of which the time period for the Supplier to comply with this Paragraph shall be extended as determined by the Appropriate Authority (acting reasonably) but shall in any case be no longer than six months after the Corporate Change Event. During a Corporate Change Event Grace Period the Supplier shall regularly and fully engage with the Appropriate Authority to enable it to understand the nature of the Corporate Change Event and the Appropriate Authority shall reserve the right to terminate a Corporate Change Event Grace Period at any time if the Supplier fails to comply with this Paragraph; or
- (b) not required pursuant to Paragraph 3.10;

3.8.3 within 30 days of the date that:

- (a) the credit rating(s) of each of the Supplier and its Parent Undertakings fail to meet any of the criteria specified in Paragraph 3.10; or
- (b) none of the credit rating agencies specified at Paragraph 3.10 hold a public credit rating for the Supplier or any of its Parent Undertakings; and

3.8.4 in any event, within 6 months after each Accounting Reference Date or within 15 months of the date of the previous Assurance received from the Appropriate Authority (whichever is the earlier), unless:

- (a) updated CRP Information has been provided under any of Paragraphs 3.8.1 3.8.2 or 3.8.3 since the most recent Accounting Reference Date (being no more than 12 months previously) within the timescales that would ordinarily be required for the provision of that information under this Paragraph 3.8.4; or

(b) not required pursuant to Paragraph 3.10.

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

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

3.10.1 Aa3 or better from Moody's;

3.10.2 AA- or better from Standard and Poors;

3.10.3 AA- or better from Fitch;

the Supplier will not be required to provide any CRP Information unless or until either (i) a Financial Distress Event occurs (unless the Supplier is relieved of the consequences of the Financial Distress Event due to credit ratings being revised upwards) or (ii) the Supplier and its Parent Undertakings cease to fulfil the criteria set out in this Paragraph 3.10, in which cases the Supplier shall provide the updated version of the CRP Information in accordance with paragraph 3.8.

3.11 Subject to Paragraph 5, where the Supplier demonstrates to the reasonable satisfaction of the Appropriate Authority or Appropriate Authorities that a particular item of CRP Information is highly confidential, the Supplier may, having orally disclosed and discussed that information with the Appropriate Authority or Appropriate Authorities, redact or omit that information from the CRP Information provided that if a Financial Distress Event occurs, this exemption shall no longer apply and the Supplier shall promptly provide the relevant information to the Appropriate Authority or Appropriate Authorities to the extent required under Paragraph 3.8.

4. Termination Rights

- 4.1 The Buyer shall be entitled to terminate the Call-Off Contract if the Supplier is required to provide CRP Information under Paragraph 3 and either:
 - 4.1.1 the Supplier fails to provide the CRP Information within 4 months of the Start Date if this is a Critical Service Contract or otherwise within 4 months of the Appropriate Authority's or Appropriate Authorities' request; or
 - 4.1.2 the Supplier fails to obtain an Assurance from the Appropriate Authority or Appropriate Authorities within 4 months of the date that it was first required to provide the CRP Information under the Call-Off Contract, which shall be deemed to be an event to which Clause 18.4 applies.

5. Confidentiality and usage of CRP Information

- 5.1 The Buyer agrees to keep the CRP Information confidential and use it only to understand the implications of an Insolvency Event of the Supplier and/or Supplier Group members on its UK Public Sector Business and/or services in respect of CNI and to enable contingency planning to maintain service continuity for end users and protect CNI in such eventuality.
- 5.2 Where the Appropriate Authority is the Cabinet Office Markets and Suppliers Team, at the Supplier's request, the Buyer shall use reasonable endeavours to procure that the Cabinet Office enters into a confidentiality and usage agreement with the Supplier containing terms no less stringent than those placed on the Buyer under paragraph 5.1 and incorporated Framework Agreement clause 34.
- 5.3 The Supplier shall use reasonable endeavours to obtain consent from any third party which has restricted the disclosure of the CRP Information to enable disclosure of that information to the Appropriate Authority or Appropriate Authorities pursuant to Paragraph 3 subject, where necessary, to the Appropriate Authority or Appropriate Authorities entering into an appropriate confidentiality agreement in the form required by the third party.

- 5.4 Where the Supplier is unable to procure consent pursuant to Paragraph 5.3, the Supplier shall use all reasonable endeavours to disclose the CRP Information to the fullest extent possible by limiting the amount of information it withholds including by:
- 5.4.1 redacting only those parts of the information which are subject to such obligations of confidentiality;
 - 5.4.2 providing the information in a form that does not breach its obligations of confidentiality including (where possible) by:
 - (a) summarising the information;
 - (b) grouping the information;
 - (c) anonymising the information; and
 - (d) presenting the information in general terms
- 5.5 The Supplier shall provide the Appropriate Authority or Appropriate Authorities with contact details of any third party which has not provided consent to disclose CRP Information where that third party is also a public sector body and where the Supplier is legally permitted to do so.

ANNEX 1: EXPOSURE: CRITICAL CONTRACTS LIST

1 The Supplier shall:

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

- (a) are with any UK public sector bodies including: central government departments and their arms-length bodies and agencies, non-departmental public bodies, NHS bodies, local buyers, health bodies, police fire and rescue, education bodies and the devolved administrations;
- (b) are with any private sector entities where the end recipient of the service, goods or works provision is any of the bodies set out in Paragraph 1.1(a) of this Annex 1 and where the member of the Supplier Group is acting as a key sub-contractor under the contract with the end recipient; or
- (c) involve or could reasonably be considered to involve CNI;

1.2 provide the Appropriate Authority with a copy of the latest version of each underlying contract worth more than £5m per contract year and their related key sub-contracts, which shall be included as embedded documents within the CRP Information or via a directly accessible link

ANNEX 2: CORPORATE RESOLVABILITY ASSESSMENT (STRUCTURAL REVIEW)

- 1 The Supplier shall:
 - 1.1 provide sufficient information to allow the Appropriate Authority to understand the implications on the Supplier Group's UK Public Sector Business and CNI agreements listed pursuant to Annex 1 if the Supplier or another member of the Supplier Group is subject to an Insolvency Event;
 - 1.2 ensure that the information is presented so as to provide a simple, effective and easily understood overview of the Supplier Group; and
 - 1.3 provide full details of the importance of each member of the Supplier Group to the Supplier Group's UK Public Sector Business and CNI agreements listed pursuant to Annex 1 and the dependencies between each.

ANNEX 3: Financial information AND COMMENTARY

- 1 The Supplier shall:
 - 1.1 provide sufficient financial information for the Supplier Group level, contracting operating entities level, and shared services entities' level to allow the Appropriate Authority to understand the current financial interconnectedness of the Supplier Group and the current performance of the Supplier as a standalone entity; and
 - 1.2 ensure that the information is presented in a simple, effective and easily understood manner.
- 2 For the avoidance of doubt the financial information to be provided pursuant to Paragraph 1 of this Annex 3 should be based on the most recent audited accounts for the relevant entities (or interim accounts where available) updated for any material changes since the Accounting Reference Date provided that such accounts are available in a reasonable timeframe to allow the Supplier to comply with its obligations under this Schedule. If such accounts are not available in that timeframe, to the extent permitted by Law financial information should be based on unpublished unaudited accounts or management accounts (disclosure of which to the Appropriate Authority remains protected by confidentiality).

Annex 4

Annex 4: Section 1 – Information Security

Information Security Terms and Conditions

Security Conditions:

Guidance for UK Contractors on the Protection of UK Assets marked as OFFICIAL - Sensitive

1. The term "Authority" means the Contracting Authority.

Security Grading

2. The Authority shall issue a Security Aspects Letter which shall define the OFFICIAL - SENSITIVE information that is furnished to the Contractor, or which is to be developed by it, under this Contract. The Contractor shall mark all OFFICIAL - SENSITIVE documents which it originates or copies during the Contract clearly with the OFFICIAL - SENSITIVE classification.

Official Secrets Acts

3. The Contractor's attention is drawn to the provisions of the Official Secrets Acts 1911 to 1989 in general, and to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular. The Contractor shall take all reasonable steps to make sure that all individuals employed on any work in connection with the Contract (including sub-contractors) have notice that these statutory provisions, or any others provided by the Authority, apply to them and shall continue so to apply after the completion or earlier termination of the Contract.

Protection of OFFICIAL - SENSITIVE Information

4. The Contractor shall protect OFFICIAL - SENSITIVE information provided to it or generated by it in accordance with the requirements detailed in this Security Condition and any other conditions that may be specified by the Authority. The Contractor shall take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.

5. OFFICIAL - SENSITIVE information shall be protected in a manner to avoid unauthorised access. The Contractor shall take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.

6. All OFFICIAL - SENSITIVE material including documents, media and other material shall be physically secured to prevent unauthorised access. When not in use OFFICIAL - SENSITIVE documents/material shall be stored under lock and key. As a minimum, when not in use, OFFICIAL - SENSITIVE material shall be stored in a lockable room, cabinets, drawers or safe and the keys/combinations are themselves to be subject to a level of physical security where applicable and control.

7. Disclosure of OFFICIAL - SENSITIVE information shall be strictly in accordance with the "need to know" principle. Except with the written consent of the Authority, the Contractor shall not disclose any of the classified aspects of the Contract detailed in the Security Aspects Letter other than to a person directly employed by the Contractor or sub-Contractor, or Service Provider.

8. Any samples, patterns, specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the Contract remain the property of the Authority and shall be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 26.

Access

9. Access to OFFICIAL - SENSITIVE information shall be confined to those individuals who have a "need-to-know" and whose access is essential for the purpose of his or her duties.

10. The Contractor shall ensure that all individuals having access to OFFICIAL - SENSITIVE information have undergone basic recruitment checks. Contractors shall apply the requirements of HMG Baseline Personnel Security Standard (BPSS) for all individuals having access to OFFICIAL - SENSITIVE information. Further details and the full requirements of

the BPSS can be found at the GOV.UK website at: <https://www.gov.uk/government/publications/security-policy-framework>

Hard Copy Distribution of Information

11. OFFICIAL - SENSITIVE documents shall be distributed, both within and outside company premises, in such a way as to make sure that no unauthorised person has access. It may be sent by ordinary post or Commercial Couriers in a single envelope. The words OFFICIAL - SENSITIVE shall **not** appear on the envelope. The envelope should bear a stamp or details that clearly indicate the full address of the office from which it was sent.

Advice on the distribution of OFFICIAL - SENSITIVE documents abroad or any other general advice including the distribution of OFFICIAL - SENSITIVE hardware shall be sought from the Authority.

Electronic Communication, Telephony and Facsimile Services

12. OFFICIAL - SENSITIVE information shall normally be transmitted over the internet encrypted using a 256 AES encryption.

Exceptionally, in urgent cases, OFFICIAL - SENSITIVE information may be emailed unencrypted over the internet **only** where there is a strong business need to do so and only with the **prior** approval of the Authority.

13. OFFICIAL - SENSITIVE information shall only be sent when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions and subject to any explicit limitations that the authority shall require. Such limitations, including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the material.

14. OFFICIAL - SENSITIVE information may be discussed on fixed and mobile types of telephone within the UK, but not with (or within) earshot of) unauthorised persons.

15. OFFICIAL - SENSITIVE information may be faxed to UK recipients.

Use of Information Systems

16. The detailed functions that must be provided by an IT system to satisfy the minimum requirements described below cannot be described here; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.

17. As a general rule, any communication path between an unauthorised user and the data can be used to carry out an attack on the system or be used to compromise or ex-filtrate data.

18. The following describes the minimum security requirements for processing and accessing OFFICIAL - SENSITIVE information on IT systems.

a. Access: Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of "least privilege" shall be applied to System Administrators. Users of the IT System (Administrators should not conduct „standard“ User functions using their privileged accounts.

b. Identification and Authentication (ID&A): All systems shall have the following functionality:

(1) Up-to-date lists of authorised users.

(2) Positive identification of all users at the start of each processing session.

c. Passwords: Passwords are part of most ID&A Security Measures. Passwords shall be „strong“ using an appropriate method to achieve this, for example, including numeric and "special" characters (if permitted by the system) as well as alphabetic characters.

d. Internal Access Control: All systems shall have internal Access Controls to prevent unauthorised users from accessing or modifying the data.

e. Data Transmission: Unless the Authority authorises otherwise, OFFICIAL - SENSITIVE information shall be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet, using a Foundation Grade product or equivalent as described in paragraph 12 above.

f. Security Accounting and Audit: Security relevant events fall into two categories, namely legitimate events and violations.

(1) The following events shall always be recorded:

- I. All log on attempts, whether successful or failed.
- II. Log off (including time out where applicable).
- III. The creation, deletion or alteration of access rights and privileges.
- IV. The creation, deletion or alteration of passwords.

(2) For each of the events listed above, the following information is to be recorded:

- V. Type of event
- VI. User ID
- VII. Date & Time
- VIII. Device ID

The accounting records shall have a facility to provide the System Manager with a hard copy of all or selected activity. There shall also be a facility for the records to be printed in an easily readable form. All security records are to be inaccessible to users without a need to know.

If the operating system is unable to provide this then the equipment shall be protected by physical means when not in use, i.e. locked away or the hard drive removed and locked away.

g. Integrity & Availability: The following supporting measures shall be implemented:

- 1. Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations)
- 2. Defined Business Contingency Plan
- 3. Data backup with local storage
- 4. Anti-Virus Software (Implementation, with updates, of an acceptable industry standard Anti-virus software).
- 5. Operating systems, applications and firmware should be supported
- 6. Patching of Operating Systems and Applications used shall be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk shall be documented.

h. Logon Banners: Wherever possible, a "Logon Banner" shall be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring.

i. suggested format for the text depending on national legal requirements could be: "Unauthorised access to this computer system may constitute a criminal offence".

j. Unattended Terminals: Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, or systems must activate a password protected screen saver after 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.

k. Internet Connections: Computer systems shall not be connected direct to the Internet or „untrusted“ systems unless protected by a firewall (a software based personal firewall is the minimum) which is acceptable to the Authority's Principal Security Advisor.

l. Disposal: Before IT storage media (e.g. disks) are disposed of, an erasure product shall be used to overwrite the data. This is a more thorough process than deletion of files, which does not remove the data.

Laptops

19. Laptops holding any supplied or contractor generated OFFICIAL - SENSITIVE information are to be encrypted using a Foundation Grade product of equivalent as described in paragraph 12 above.

20. Unencrypted laptops not on a secure site² are to be recalled and only used or stored in an appropriately secure location until further notice or until approved full encryption is installed. Where the encryption policy cannot be met, a Risk Balance Case that fully explains why the policy cannot be complied with, and the mitigation plan, which should explain any limitations on the use of the system, is to be submitted to the Authority for consideration. Unencrypted

laptops and drives containing personal data are not to be taken outside of secure sites. For the avoidance of doubt, the term "drives" includes all removable, recordable media (e.g. memory sticks, compact flash, recordable optical media (e.g. CDs and DVDs), floppy discs and external hard drives.

21. Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.

22. Portable CIS devices are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven, the CIS is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

² *Secure Sites are defined as either Government premises or a secured office on the contractor premises*

Loss and Incident Reporting

23. The contractor shall immediately report any loss or otherwise compromise of OFFICIAL - SENSITIVE information to the Authority. Any security incident involving OFFICIAL - SENSITIVE information shall be immediately reported to the Authority.

Sub-Contracts

24. The use of any sub-contractors must be stated in the Data Protection Impact Assessment (DPIA). If during the course of the contract it is decided to sub-contract work this must be reflected in an updated DPIA and this be approved by the Data Protection Officer of the CMA.

If the Sub-contract is approved, the Authority shall provide the Contractor with the security conditions that shall be incorporated within the Sub-contract document.

Publicity Material

25. Contractors wishing to release any publicity material or display hardware that arises from this contract shall seek the prior approval of the Authority. Publicity material includes open publication in the contractor's publicity literature or website or through the media; displays at exhibitions in any country; lectures or symposia; scientific or technical papers, or any other occasion where members of the general public may have access to the information even if organised or sponsored by the Authority or any other government department.

Destruction

26. As soon as no longer required, OFFICIAL - SENSITIVE information/material shall be destroyed in such a way as to make reconstitution unlikely, for example, by burning, shredding or tearing into small pieces. Advice shall be sought from the Authority when information/material cannot be destroyed or, unless already authorised by the Authority, when its retention is considered by the Contractor to be necessary or desirable. Unwanted OFFICIAL - SENSITIVE information/material which cannot be destroyed in such a way shall be returned to the Authority.

Interpretation/Guidance

27. Advice regarding the interpretation of the above requirements should be sought from the Authority.

Audit

28. Where considered necessary by the Authority, the Contractor shall provide evidence of compliance with this Security Condition and/or permit the inspection of the Contractors processes and facilities by representatives of the Authority to ensure compliance with these requirement.

SECURITY ASPECTS LETTER

1. The above work arises from a United Kingdom government contract and will involve your company holding UK classified material. It shall be a condition of the Contract that this material must be protected. The standard of protection required has been notified varies with the level of classification. Material passed to you will bear the classification appropriate to it. However to assist you in allocating any necessary classification to material which your company may produce during the course of the Contract and thus enable you to provide the appropriate degree of protection to it, this letter formally advises you of the correct classification to apply to the various aspects of the Contract.

2. The aspects of the Contract which require to be classified are:

ASPECTS	CLASSIFICATION
Commercially sensitive information	Official sensitive
Internal communications within the CMA	Official / Official sensitive
External communications within the CMA and other stakeholders	Official / Official sensitive
Personal data	Official sensitive

3. If the Contract contains a Condition of Clause referring to "Secret Matter" this Secret matter is defined as the Aspects listed above.

4. You are requested to acknowledge receipt of this letter and to confirm that the level of classification associated with the various aspects listed above have been brought to the attention of the person directly responsible for the security of this Contract, that they are fully understood, and that the required security controls in the contract security conditions can and shall be taken to safeguard the material concerned.

5. If you have any difficulty in interpreting the meaning of the above aspects or in safeguarding the materials, please contact [REDACTED], immediately on the following:

[REDACTED] or by telephone: [REDACTED]

This section is agreed to in the acknowledgement section of this document

Annex 4: Section 2 – Supplementary Terms and Conditions of Contract:

Supplementary Terms and Conditions of Contract	
1.	Authorised Representative
1.1.	The below person (including any successor in office from time to time of such person) is authorised to act as the CMA's Representative on all matters concerning this Contract:
1.2.	Each of the CMA and the Contractor may from time to time by notice in writing to the other party appoint another person to act as its authorised representative. Both parties shall use their reasonable endeavours to ensure that any such substitutions and or additions do not have any adverse impact on the Services.
2.	Indemnities and Insurance
2.1.	The Contractor shall hold harmless and indemnify the CMA on demand from and against all claims, demands, proceedings, actions, damages, costs (including legal costs), expenses and any other liabilities arising from claims made by the CMA, in respect of any death or personal injury, or loss or destruction of or damage to property, or any other loss, destruction or damage, including but not limited to financial losses which are caused, directly by the breach of contract or breach of duty (whether in negligence, tort, statute or otherwise) of the Contractor.
2.2.	The Contractor shall be liable to the CMA for any direct loss, damage, destruction, injury or expense, (and including but not limited to loss or destruction of or damage to the CMA's property, which includes data) arising from the Contractor's breach of contract or duty (whether arising in negligence, tort, statute or otherwise).
2.3.	The Contractor shall effect with a reputable insurance company a policy or policies of insurance providing an adequate level of cover in respect of all risks which may be incurred by the Contractor in respect of the indemnities provided under the Contract, which in any event shall not be less than the G-Cloud 14 framework rates, and shall at the request of the CMA produce the relevant policy or policies together with receipt or other evidence of payment of the latest premium due there under.
2.4.	Nothing in these Conditions or in any part of the Contract shall impose any liability on any member of the staff of the CMA or its representatives in their personal capacity.
2.5.	The Contractor shall indemnify the CMA against all proceedings, actions, claims, demands, costs (including legal costs), charges, expenses and any other liabilities arising from or incurred by reason of any infringement or alleged infringement of any third party's Intellectual Property Rights used by or on behalf of the Contractor for the purpose of the Contract, providing that any such infringement or alleged infringement is not knowingly caused by, or contributed to, by any act of the CMA.
2.6.	The CMA shall indemnify the Contractor against all proceedings, actions, claims, demands, costs (including legal costs), charges, expenses and any other liabilities arising from or incurred by reason of any infringement or alleged infringement of any third party's Intellectual Property Rights used at the request of the CMA by the Contractor in the course of providing the Services, providing that any such infringement or alleged infringement is not knowingly caused by, or contributed to by, any act of the Contractor.
2.7.	Except in relation to death or personal injury as referred to in Condition 2.1 and subject to Conditions 2.5 and 2.6 the amount of liability under this Condition shall in no event exceed the amount of twelve (12) calendar months' worth of the Fees..
2.8.	The CMA shall not be liable under to pay any sum which: <ul style="list-style-type: none"> • was claimable under insurance held by the Contractor, and the Contractor has failed to make a claim on its insurance, or has failed to make a claim in accordance with the procedural requirements of the insurance policy; • when added to any sums paid or due to the Contractor under the Contract exceeds the total sum that would have been payable to the Contractor if the Contract had not been terminated prior to the expiry of the Contract Duration; or • is a claim by the Contractor for loss of profit or any indirect or consequential loss, due to early termination of the Contract.
3.	Conflicts of Interest
3.1.	The Contractor shall disclose to the CMA's Representative as soon as is reasonably practical after becoming aware of any actual or potential conflict of interest relating to provision of the Services by the Contractor or any event or matter

(including without limitation its reputation and standing) of which it is aware or anticipates may justify the CMA taking action to protect its interests.

4. Survival of the Contract

4.1. Insofar as any of the rights and obligations of the parties in this Contract shall or may be exercised after expiry or termination of the Contract, the provisions of this Contract conferring such rights and powers shall survive and remain in full force and effect notwithstanding such termination or expiry..

5. Working Time Directive

5.1. The Contractor shall ensure that the Working Time Directive Employment Regulations shall be applied in the proper manner to all personnel supplied via this Contract.

5.2. The Contractor shall ensure that commensurate with good employment practices and policies observed by the CMA, that all employment legislation is applied appropriately to all workers employed in providing the Services.

6. Observance of Statutory Requirements

6.1. The Contractor insofar as it is legally liable shall comply with all statutory requirements to be observed and performed in connection with the Contract.

7. Equal Opportunities and Harassment

7.1. The Contractor shall adopt a policy to comply with the requirements of the Race Relations Act 1976, the Race Relations (Amendment) Act 2000, the Employment Equality (Religion or Belief) Regulations 2003, the Sex Discrimination Act 1975 as amended, Equal Pay Act 1970, Employment Equality (Sexual Orientation) Regulations 2003, Sex Discrimination (Gender Reassignment) Regulations 1999, and the Disability Discrimination Act 1995 and the Disability Discrimination Act 2005, and accordingly, shall not treat one individual or group of people less favourably than others because of colour, race, nationality, ethnic origin, religion, gender, sexual orientation or disability and, further, shall seek to promote equality among its workers and generally. The Contractor shall note the CMA's current and future obligations under these Acts and under the Data Protection Act 2018, Freedom of Information Act 2000, Human Rights Act 1998, and any codes of practice and best practice guidance issued by the Government and the appropriate enforcement agencies.

7.2. The Contractor shall comply with the above legislation in so far as it places obligations upon the Contractor in the performance of its obligations under this Contract. The Contractor shall facilitate the CMA's compliance with the CMA's obligations under these provisions and comply with any request from the CMA for that purpose.

7.3. In the event of any finding of unlawful racial, disability or sexual discrimination being made against the Contractor by any court or industrial tribunal, or of an adverse finding in any formal investigation by the Equality and Human Rights Commission the Contractor shall take appropriate steps to prevent repetition of the unlawful discrimination and shall on request provide the CMA with details of any steps taken.

7.4. The Contractor shall set out its policies on race relations, sex discrimination and disability discrimination:

- in instructions to those concerned with recruitment, training and promotion;
 - in documents available to its personnel, recognised trade unions or other representative groups of its personnel;
- and
- in recruitment advertisements and other literature.

7.5. The Contractor shall, on request provide the CMA with copies of its policies, examples of the instructions and other documents, recruitment advertisements and other literature.

7.6. The Contractor shall provide such information as the CMA may reasonably request for the purpose of assessing the Contractor's compliance with this Condition 8.

7.7. The Contractor shall take all reasonable steps to ensure that Contractor's personnel engaged in the performance of the Contract do not act towards either CMA staff or members of the public in a manner that could amount to harassment on any of the grounds mentioned in 8.1. In the event of any finding of unlawful discrimination being made against the Contractor by any court or tribunal, or of any adverse finding in any formal investigation, the Contractor shall take appropriate steps to prevent repetition of the unlawful discrimination and shall, on request, provide the CMA with details of any steps taken.

8. Payment

8.1. All invoices must be sent, quoting a valid purchase order number, to: The Competition and Markets Authority, Finance Team, The Cabot, 25 Cabot Square, London E14 4QZ. Within [10] working days of receipt of your countersigned

copy of this letter, we will send you a Purchase Order (PO) with unique PO number. You must be in receipt of a valid PO number before submitting an invoice.

8.2. To avoid delay in payment it is important that the invoice is compliant and that it includes a valid PO number, PO number item number (if applicable) and the details (name and telephone number) of your customer contact (i.e. Contract Manager). Non-compliant invoices will be sent back to you, which may lead to a delay in payment. If you have a query regarding an outstanding payment please contact our Accounts Payable section either by email to

██████████ or by telephone ██████████ between 09:00-17:00 Monday to Friday.

9. Relevant Conviction

9.1. The CMA may require the Contractor to ensure that any person employed in the provision of Services has undertaken a Disclosure and Barring Service check. The Contractor shall ensure that no person who discloses that he/she has a conviction that is relevant to the nature of any Services, relevant to the work of the CMA, or is of a type otherwise advised by the CMA (each such conviction a "Relevant Conviction"), or is found by the Supplier to have a Relevant Conviction (whether as a result of a police check, a Disclosure and Barring Service check or otherwise) is employed or engaged in the provision of any part of the Services.

10. Publicity

10.1. The service provider agrees not to disclose the identity of CMA as a client of the service provider, nor to use the CMA's name nor refer to the CMA directly or indirectly in any advertisement or other publication without receiving the CMA's prior written approval for such use or reference and to the form and context in which the reference to the CMA is to appear.

10.2. The service provider shall abide by any conditions or limitations imposed by the CMA in such approval, if given.

10.3. The service provider further agrees not to disclose the existence of this contract, or the nature of the relationship established by this contract.

Annex 4: Section 3 – Confidentiality and Security Requirements:

Confidentiality and Security Requirements

1. The secrecy and security aspects of the Competition & Markets Authority's work are governed by section 5 of the Official Secrets Act 1989, section 101 of the Telecommunications Act 1984, section 206 of the Water Industry Act 1991, section 74 of the Airports Act 1986, section 197 of the Broadcasting Act 1990, section 145 of the Railways Act 1993, Article 49 of the Airports (Northern Ireland) Order 1994, sections 348, 350(5) and 352 of the Financial Services and Markets Act 2000, Schedule 7 of the Postal Services Act 2000, section 105 of the Utilities Act 2000, Schedule 9 of the Transport Act 2000, Part 9 of the Enterprise Act 2002, Article 63 of the Energy (Northern Ireland) Order 2003, section 393 of the Communications Act 2003 and Article 265 of The Water and Sewerage Services (Northern Ireland) Order 2006 (the Acts). Contractors shall be bound by the provisions of the Acts. Contractors should ensure that they fully understand the serious consequences that which may follow from a breach of any of these confidentiality requirements.

2. The confidentiality provisions of the Acts constitute a set of general restrictions on the disclosure of information obtained under the Acts in respect of particular businesses except when this is necessary for the purposes of the Act or for certain other prescribed purposes. Criminal prosecution is possible where unauthorised disclosure takes place. Most of the documents handled by the CMA fall within the scope of these statutory restrictions on disclosure and as 'sensitive documents' require the protection of effective security control and of strict observance of security rules. Contractors shall be expected to follow the CMA's security rules and these shall be discussed fully with them prior to commencement of the service.

3. Part V of the Criminal Justice Act 1993 also applies to information obtained in the course of CMA inquiries. It is a criminal offence under that legislation for members of a Contractor's staff to deal, or to encourage others to deal, in securities about which they hold inside information (i.e. unpublished price sensitive information relating to particular securities), obtained by virtue of their work for the CMA, or to disclose such information otherwise than in the proper performance of their work.

4. Contractors shall be responsible for ensuring that all staff employed in connection with any aspect of the service do not divulge any information obtained in, or as a result of, their work for the Competition and Markets Authority, except in the course of duty. The requirement not to divulge information includes not divulging information to other members of the Contractors' staff. Contractors shall also be responsible for ensuring that members of their staff are aware of and abide by the confidentiality provisions of the Acts and sign a witnessed declaration of the form set out in the Acknowledgement section at the end of this document. This requirement shall include all support staff who may be involved in system administration or other duties which require them to be given access to any part of the Competition and Markets Authority network. A copy of this signed document shall be sent to the Contract Manager.

This section is agreed to in the acknowledgement section of this document

Annex 4: Section 4 – Confidentiality Undertaking:

CONFIDENTIALITY UNDERTAKING, THE COMPETITION AND MARKETS AUTHORITY

I understand that in any work for 'the CMA' which I perform I shall be in possession of information which is held in confidence and which must not be disclosed without lawful authority. I am aware that the legislation referred to below provides for criminal prosecution where unauthorised disclosure takes place, and that on conviction a person may be fined or imprisoned. I am also aware that, in law, I owe duties of confidentiality to the CMA.

I accept that I must not communicate, orally or in writing, any information gained by me as a result of my work for the CMA to any person other than a person to whom it is my duty to communicate it without the consent of the Chief Executive of the CMA (or an authorised member of her staff). In the case of information with respect to any particular trade or business, I accept that the consent of the person carrying on that trade or business is required also. I accept that articles of any description prepared for publication or discussion in any written form or for broadcasting are covered by these conditions.

I also acknowledge that Part 9 of the Enterprise Act 2002 and Part V of the Criminal Justice Act 1993 apply to me and that it is a criminal offence to (1) use or disclose information in contravention of Part 9 of the Enterprise Act 2002 as they apply to me and (2) deal, or to procure others to deal, in securities about which I hold unpublished price sensitive information when engaged in work for or on behalf of the CMA.

This section is agreed to in the acknowledgement section of this document

Annex 4: Section 5 – Conflicts of interest:

CONFLICTS OF INTEREST IN RELATION TO CONTRACTORS AND CONTRACTORS' STAFF

Summary

1. Contractors and their staff must disclose any interests which might give rise to a conflict or potential conflict to the CMA before entering into a contract with the CMA. The CMA will consider whether the potential conflict causes concern and what action (if any) should be taken. It may be necessary to require the disposal of an interest in order for the CMA to be able to enter into a contract.

Detail

2. When a Contractor is approached with a view to entering into a contract or call-off with the CMA, the Contractor must disclose to the CMA any potential conflict of interest of which it is aware, or becomes aware, affecting any of the following:

- a) the Contractor, their spouse, or partner (other than a spouse) and dependents;
- b) all personnel of the Contractor whose involvement on a contract with the CMA is not purely mechanical or clerical; and
- c) all directors, partners and other senior personnel of a Contractor with equivalent responsibilities even though they are not involved in a contract with the CMA.

3. If the Contractor has any doubts as to whether or not there exists an interest which may give rise to a conflict, these doubts must also be disclosed.

4. In this annex the following terms have the meanings set out below:

a) "relevant individuals" means persons within sub-paragraphs 2 (a) to (c) above, together with their spouses, partners (other than a spouse) and dependents;

b) "the reference companies" means any company (incorporated or unincorporated), partnership, business or individual that is the subject of the reference relating to the Contract or Call-off to be awarded to the Contractor;

c) "the relevant companies" means any company (incorporated or unincorporated), partnership, business or individual who is a competitor, customer or supplier of any reference companies.

d) "shareholding" includes:

- (i) shares, whether bearing a right to vote or not;
- (ii) stock or debentures; and
- (iii) options and similar rights;
- (iv) in each case whatever the value of the holding and whether held as trustee or beneficially, (for example under a family trust or a Personal Equity Plan). Holdings in unit trusts, investment trusts, unit linked policies or similar arrangements under which the investor has interests in a large number of enterprises would not normally give rise to a potential conflict of interest, unless any company involved in the arrangements were itself affected by the inquiry. However, if the trust or arrangement specialises in investing in a particular industry which is affected by the reference or if the investor believes that there is a real possibility of the value of the investment being affected by the outcome of the reference, the interest should be disclosed to the CMA.

5. The requirement under paragraph 3 to disclose any potential conflict of interest includes a requirement to disclose any relationship which may give an appearance of bias on the part of the Contractor or its staff including but not limited to:

- a. the Contractor's present or past contractual relationship with any of the reference companies;
- b. the Contractor's present or past contractual relationship with any of the relevant companies;
- c. the Contractor's or relevant individuals' shareholding or partnership in, ownership (whether full or partial) or directorship of, or employment by:

- (i) the reference companies;
 - (ii) the relevant companies; and
 - (iii) any enterprise the value of whose shares may be affected by the outcome of the reference (e.g. an enterprise in the same industry).
 - d. the Contractor's present or past contractual relationship with, or the Contractor's, or relevant individuals', employment by the relevant regulator (if applicable in relation to the reference);
 - e. the management of the investment of a shareholding or other interest of a person for which the Contractor, or any relevant individual, is responsible; and
 - f. a recent personal or family involvement with the reference companies or the relevant companies e.g. a substantial shareholding or other interest which has recently been disposed of.
6. Share accounts with a building society would not need to be disclosed except, for example, where they entitled the holder to a "perk" in the event of a merger. Similarly, bank accounts would not normally need to be disclosed in a reference involving the bank, though they should be disclosed where a person wishes to obtain or renegotiate a loan or overdraft.
7. A potential conflict of interest may arise in other circumstances, such as where there is a business relationship with an enterprise affected by the reference or any other close relationship with a person whose affairs may be affected by the reference. **In case of doubt the Contractor or relevant individual should disclose the interest.**
8. An interest as a consumer would not need to be disclosed, in normal circumstances, where the value of the goods or services obtained is small or most individuals are consumers (e.g. in the case of a market investigation into the supply of milk, salt or bread). If however the interest is that of a minority class of consumer there might be a conflict. This might be the case if, for example, an individual, his or her spouse, or child, were a coeliac and as such required gluten free products which were produced by companies involved in a merger reference.
9. The Contractor should check and relevant individuals as defined in paragraph 4 above should be required by the Contractor to check (if they are not already confident of the facts) their own shareholdings and shareholdings held on their behalf. They should also check, information which has been provided to them, e.g. as trustees or a holder of a specialised unit trust and whether they are aware in general terms of any conflict of interest.
10. The CMA will decide whether anything which has been disclosed as a potential conflict of interest constitutes an actual conflict in the particular circumstances. In some circumstances it may suffice for an interest which does give rise to a conflict to be disposed of in the period between public announcement of the reference and distribution of relevant papers, (subject to the approval of the CMA). In some circumstances it may be sufficient simply to inform the parties involved in the inquiry or likely to be involved of the interest (be it a shareholding or other interest).

CONFLICTS OF INTEREST STATEMENT

THE COMPETITION AND MARKETS AUTHORITY

1. We confirm that there is no conflict of interest that might give rise to a risk of challenge in the courts to the inquiry on the ground of bias (whether actual or apparent). The acceptance of the following terms and conditions shall be taken as confirmation that no such conflicts of interest exist.
2. We shall ensure that actual or even potential conflicts do not arise during the course of the inquiry. In particular:
 - a) For the duration of the inquiry we shall not undertake or actively seek any work for any organisation that is directly related to the subject of the inquiry. We agree that work which is indirectly related other than that laid out in the contract should only be undertaken with the CMA's consent which shall not be unreasonably withheld.

b) We confirm that any individuals providing services to the inquiry, as applicable, shall not carry out any work related to the subject of the inquiry for any other client for the duration of the inquiry. However, those individuals may consult colleagues who are engaged in such work in order to obtain information from them.

c) We confirm that individuals providing services to the inquiry and their immediate families do not own or have a beneficial interest in the shares of the main parties to the inquiry or their suppliers unless such holdings are independently managed (e.g. by a unit trust or pension fund).

d) All information acquired by the individuals providing services to the inquiry shall be treated as confidential to the CMA both for the duration of the agreement and thereafter. The individuals shall not communicate it to third parties or other individuals within your firm unless it has already entered the public domain by other means. All documents supplied to us in connection with the inquiry and this agreement, copies of any part of such documents, whether in electronic or material form, and any documents prepared by us which are based on material supplied in connection with this inquiry, must be returned to the CMA at the end of the inquiry, or sooner if requested.

3. The CMA may terminate this contract at any time should it become of the opinion that an actual or potential conflict of interest on our part has arisen. We shall be entitled to remuneration on the basis set out in this letter up to the date of termination save in circumstances where we are in breach of our obligations under the terms of the contract.

4. It shall be our responsibility to ensure that no conflict of interest arises which might be said to prejudice our independence and objectivity in performing the contract. This responsibility includes all of our senior staff (e.g. directors, and partners) or our personnel whose involvement on the contract with the CMA is not purely mechanical or clerical. If we are at any time in doubt about whether any conflict of interest may exist or arise, we shall notify the CMA forthwith and comply with any directions given with a view to avoiding the conflict.

5. During the period of the contract, and for an **agreed period** after it ends, we would, **except with the prior written consent of the Contract Manager**, be debarred from working for, or having any other interest in, any of the main parties to the inquiry (which is the subject of the Contract) or any of their competitors in the relevant industry. This requirement is made to avoid conflicts of interest.

6. The acceptance of these terms and conditions shall be taken as confirming agreement on all of the above points.

This section is agreed to in the acknowledgement section of this document