



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	15
Schedule 1: Services	33
Schedule 2: Call-Off Contract charges	36
Schedule 3: Collaboration agreement	38
Schedule 4: Alternative clause	39
Schedule 5: Guarantee	43
Schedule 6: Glossary and interpretations	44
Schedule 7: UK GDPR Information	56
Annex 1: Processing Personal Data	56
Annex 2: Joint Controller Agreement	58
Schedule 8: Service Definition Document	64
Schedule 9: Corporate Resolution Planning	79
Schedule 10 : Variation Form	88

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	495914020380839
Call-Off Contract reference	CO Digital 30
Call-Off Contract title	Provision of an IT Service Management ITSM
Call-Off Contract description	<p>SaaS based IT Service Management product software solution. Featuring an intuitive UI, robust ticketing - Incident, Problem, Change and Release Management, powerful self-serve portal with service catalogue & knowledge management, reporting, integration capabilities, smart automation and GenAI capabilities.</p> <p>1 year contract + 1 year optional extension</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
Start date	30/11/2024
Expiry date	30/11/2025
Call-Off Contract value	GBP 151,530 for initial term



	<p>GBP 303,060 if optional 1 year extension is chosen.</p> <p>(Per Year GBP 151,530)</p>
Charging method	<p>BACS.</p> <p>The payment profile for this Call-Off Contract is one annual upfront payment for twelve (12) months worth of licences.</p> <p>A PO will be raised once the Contract has been signed.</p> <p>Invoices should be submitted to</p> <div style="background-color: black; width: 300px; height: 40px; margin: 5px 0;"></div> <p>All Invoices must include the PO number. Each invoice must be accompanied by a breakdown of the deliverables and services, quantity thereof, applicable unit charges and total charge for the invoice period, in sufficient detail to enable the Customer to validate the invoice.</p>
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	Cabinet Office Digital 
To the Supplier	Freshworks Inc. 
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: Senior Commercial Manager

Name: [REDACTED]
Email: [REDACTED]
Phone: [REDACTED]

For the Supplier:

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

Call-Off Contract term

Start date	This Call-Off Contract Starts on 30.11.2024 and is valid for 12 months .
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 one periods of up to 12 months, by giving the Supplier 60 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> <p>Lot 2: Cloud software</p>
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:</p> <p>Detailed in Schedule 1.</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
Additional Services	Not applicable
Location	<p>Any data that Freshworks process for the Buyer as a data processor will be stored in the EU. However, Freshworks may also process certain data about Buyer or its users as a data controller, including in countries outside of the EU, in accordance with Freshworks privacy notice available at https://www.freshworks.com/privacy/</p>
Quality Standards	<p>The quality standards required for this Call-Off Contract is mentioned in the Service Definition Document attached under Annexure 8 of the Call-off Contract.</p>
Technical Standards:	<p>The technical standards used as a requirement for this Call-Off Contract is mentioned in the Service Definition</p>

	Document attached under Annexure 8 of the Call-off Contract.
Service level agreement:	The service level and availability criteria required for this Call-Off Contract is mentioned in the Service Definition Document attached under Annexure 8 of the Call-off Contract and shown below:
Onboarding	The onboarding plan for this Call-Off Contract is mentioned in the Service Definition Document attached under Annexure 8 of the Call-off Contract.

Offboarding	The offboarding plan for this Call-Off Contract is mentioned in the Service Definition Document attached under Annexure 8 of the Call-off Contract.
Collaboration agreement	Not applicable.

Limit on Parties' liability	<p>The annual total liability of either Party for all Property Defaults will not exceed 100% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.</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 100% 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 100% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.</p>
Insurance	<p>The insurance(s) required will be:</p> <ul style="list-style-type: none">• A minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract• professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law)• employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Force Majeure	<p>A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 30 consecutive days.</p>

Audit	<p>1.1 Supplier shall, in accordance with Data Protection Legislation, make available to Buyer on request in a timely manner such information as is necessary to demonstrate compliance by Supplier with its obligations under Data Protection Legislations.</p> <p>1.2 Supplier has obtained third-party certifications and audits set forth on our security page. Upon Buyer's written request and subject to the confidentiality obligations set forth in the Agreement, Supplier will make available to Buyer a copy of Supplier's then most recent third-party audits or certifications, as applicable.</p> <p>1.3 Supplier shall, upon reasonable notice, allow for and contribute to inspections of the Supplier's Processing of Personal Data, as well as the TOMs (including data processing systems, policies, procedures, and records), during regular business hours and with minimal interruption to Supplier's business operations. Such inspections are conducted by the Buyer, its affiliates or an independent third party on Buyer's behalf (which will not be a competitor of the Supplier) that is subject to reasonable confidentiality obligations.</p> <p>1.4 Buyer shall pay Supplier reasonable costs of allowing or contributing to audits or inspections in accordance with Section 1.5</p> <p>1.5 Where Buyer wishes to conduct more than one audit or inspection every 12 months. Supplier will immediately refer to Buyer any requests received from national data protection authorities that relate to the Supplier's Processing of Personal Data.</p> <p>1.6 Supplier undertakes to cooperate with Buyer in its dealings with national data protection authorities and with any audit requests received from national data protection authorities. Buyer shall be entitled to disclose this Data Processing Agreement or any other documents (including contracts with subcontractors) that relate to the performance of its obligations under this Agreement (commercial information may be removed).</p>
--------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Buyer's responsibilities	The Buyer shall comply with the Supplier Terms and Conditions under https://www.freshworks.com/terms/
Buyer's equipment	Not Applicable.

Supplier's information

Subcontractors or partners	<p>The following is a list of the Supplier's Subcontractors or Partners.</p> <div style="background-color: black; height: 20px; width: 400px;"></div>
-----------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------

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 one annual payment for twelve (12) months of licences as per the payments table in Schedule 2.

Invoice details	The Supplier will issue electronic invoices annually with payment upfront. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.
Who and where to send invoices to	Invoices will be sent to [REDACTED]
Invoice information required	<p>All invoices must include: All invoices must include the relevant PO and a summary of estate charges for both recurring and one-time charges.</p> <p>Primary contact name and address: Account payable address - [REDACTED]</p>
Invoice frequency	Invoice will be sent to the Buyer annually.
Call-Off Contract value	<p>The total value of this Call-Off Contract is</p> <p>GBP 151,530 for initial term</p> <p>GBP 303,060 if optional 1 year extension is chosen.</p> <p>(Per Year GBP 151,530)</p>
Call-Off Contract charges	The breakdown of the Charges is detailed in Schedule 2.

Additional Buyer terms

Performance of the Service	<p>This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones in accordance with Schedule 8 of the Call-off Contract.</p> <p>KPI's and performance monitoring details are detailed in Schedule 1.</p>
Guarantee	Not applicable.
Warranties, representations	<p>As mentioned in the Supplier's Terms and Conditions under https://www.freshworks.com/terms/</p>
Supplemental requirements in addition to the Call-Off terms	Not applicable.
Alternative clauses	<p>These Alternative Clauses, which have been selected from Schedule 4, will apply:</p> <p>Not applicable.</p>
Buyer specific amendments to/refinements of the Call-Off Contract terms	<p>Within the scope of the Call-Off Contract, the Supplier will:</p> <p>Not applicable.</p>

Personal Data and Data Subjects	Annex 1, Schedule 7 is being used.
Intellectual Property	Not applicable.
Social Value	Information was provided from the supplier on the theme of equal opportunity in the workplace. In quarterly contract review meetings these company initiatives shall be monitored and reviewed by the buyer.
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. KPI's and performance monitoring details are detailed in Schedule 1.

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	<div></div>	<div></div>
Title	<div></div>	<div></div>
Signature		
Date	<div></div>	<div></div>

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

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

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

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

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

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

3. Supply of services

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

4. Supplier staff

- 4.1 The Supplier Staff must:
 - 4.1.1 be appropriately experienced, qualified and trained to supply the Services
 - 4.1.2 apply all due skill, care and diligence in faithfully performing those duties
 - 4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
 - 4.1.4 respond to any enquiries about the Services as soon as reasonably possible

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

5. Due diligence

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

6. Business continuity and disaster recovery

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

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

7. Payment, VAT and Call-Off Contract charges

- 7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.
- 7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
- 7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.
- 7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.
- 7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.
- 7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.
- 7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.
- 7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
- 7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.
- 7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.
- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.
- 7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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

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

9. Insurance

- 9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.
- 9.2 The Supplier will ensure that:
- 9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
 - 9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit
 - 9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
 - 9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- 9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.
- 9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:
- 9.4.1 a broker's verification of insurance
 - 9.4.2 receipts for the insurance premium
 - 9.4.3 evidence of payment of the latest premiums due
- 9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:
- 9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
 - 9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances

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

10. Confidentiality

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

11. Intellectual Property Rights

- 11.1 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.
- 11.2 Neither Party shall have any right to use any of the other Party's names, logos or trademarks on any of its products or services without the other Party's prior written consent.
- 11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:
 - 11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and
 - 11.3.2 The Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer's written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.
- 11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.
- 11.5 Subject to the limitation in Clause 24.3, the Buyer shall:
 - 11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:
 - alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
 - alleging that the Buyer Data violates, infringes or misappropriate any rights of a third party;
 - arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and
 - 11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgement against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer's obligations under this Clause 11.5 shall not

apply where and to the extent such Losses or third-party claim is caused by the Supplier's breach of this Contract.

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

rights granted to the Buyer under this Call-Off Contract

Supplier's performance of the Services

use by the Buyer of the Services

11.7 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

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

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

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

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

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

other material provided by the Buyer necessary for the Services

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

12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

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

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

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

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

13. Buyer data

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

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

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

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

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

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

13.6.1 the principles in the Security Policy Framework:

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

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

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance:

<https://www.ncsc.gov.uk/collection/risk-management-collection>

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint:

<https://www.gov.uk/government/publications/technologycode-of-practice/technology-code-of-practice>

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

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

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

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

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

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

work with the Buyer on any ongoing work

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

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

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

20. Notices

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

Manner of delivery: email

Deemed time of delivery: 9am on the first Working Day after sending

Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message

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

21. Exit plan

- 21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.
- 21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.
- 21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.
- 21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.
- 21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.
- 21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from CDDO under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:
 - 21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the period on terms that are commercially reasonable and acceptable to the Buyer
 - 21.6.2 there will be no adverse impact on service continuity
 - 21.6.3 there is no vendor lock-in to the Supplier's Service at exit
 - 21.6.4 it enables the Buyer to meet its obligations under the Technology Code of Practice
- 21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.
- 21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:
 - 21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
 - 21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer

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

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

22. Handover to replacement supplier

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

23. Force majeure

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

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

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

24. Liability

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

25. Premises

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

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

26. Equipment

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

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

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

28. Environmental requirements

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

29. The Employment Regulations (TUPE)

- 29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.
- 29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to end it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:
- 29.2.1 the activities they perform

- 29.2.2 age
- 29.2.3 start date
- 29.2.4 place of work
- 29.2.5 notice period
- 29.2.6 redundancy payment entitlement
- 29.2.7 salary, benefits and pension entitlements
- 29.2.8 employment status
- 29.2.9 identity of employer
- 29.2.10 working arrangements
- 29.2.11 outstanding liabilities
- 29.2.12 sickness absence
- 29.2.13 copies of all relevant employment contracts and related documents
- 29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer.

The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

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

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

its failure to comply with the provisions of this clause

any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

- 30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.
- 30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

- 31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.
- 31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:
 - 31.2.1 work proactively and in good faith with each of the Buyer's contractors
 - 31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

- 32.1 The Buyer can request in writing a change to this Call-Off Contract using the template in Schedule 9 if it isn't a material change to the Framework Agreement or this Call-Off Contract. Once implemented, it is called a Variation.
- 32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request using the template in Schedule 9. This includes any changes in the Supplier's supply chain.
- 32.3 If either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days' notice to the Supplier.

33. Data Protection Legislation (GDPR)

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

Schedule 1: Services

To be added in agreement between the Buyer and Supplier, and will be G-Cloud Services the Supplier is capable of providing through the Platform.

Information below and found in Schedule 8.

Freshworks Service Definition Document

[495914020380839-service-definition-document-2024-05-02-1237.pdf](#)

Freshworks Terms and Conditions

[495914020380839-terms-and-conditions-2024-05-02-1237.pdf](#)

The Supplier can deliver the below 'mandatory' requirements and be working towards delivering the 'important' requirements.

ITSM Requirement	Priority
The System is to have the ability to bulk-upload and retain Asset history of all End User devices - including; device info, user info, authentication info, tickets info, OS info - including recording of Update Status reports	Mandatory
The System is to be able to handle Single Sign on across multiple domains using open authentication standards such as SAML, O-Auth or AD Authentication for all Users	Mandatory
The System is to provide and comply with ITIL Management - Incident, Change, Problem, Release, Event, Request Fulfilment and Integration with monitoring tools to trigger Event Management process	Mandatory
The System is to provide an accessible and managed Inventory and CMDB with configuration item tracking that is searchable and can be referenced to Users and tickets, Changes and Problems. Additionally, Workflow Prompts for Device and Password Release to Users based on configurable SLA's	Mandatory
The System is to enable Admins to customise and change all business Workflows or Processes used by different teams	Mandatory
The System is to enable access to progress on all current and previous requests via the Customer Portal to customers. Intelligent Workflow Management - based on set (configurable) criteria on the number of O/S tickets and Service Request Due Date	Mandatory
The System is to support Google Chrome browser, MS Edge and MS O365	Mandatory
The Customer Service Portal should include examples of preset solutions for logging tickets as defined in the Knowledge Base including the ability to load 'How To' Video tutorials	Mandatory
Allow tickets and tasks to be moved between technicians resolver groups with ease	Mandatory
The system should include examples of preset solutions for Technicians to troubleshoot as defined in the Knowledge Base	Mandatory
The system is to provide communications functionality for technicians to email or chat to requestors	Mandatory
The System is to enable both Technicians and Customers to tag multiple watchers to in a ticket (ticket following and be able to email all parties on ticket activity	Mandatory
The System is to auto-register new devices discovered in; Active Directory / WorkspaceOne / SCCM / JAMF	Mandatory

The System is to enable integration with Management tools including but not limited to JAMF, SCCM, WorkspaceOne and MS Active Directory	Mandatory
The System is to enable Technicians to search, reference and manage the Knowledge base including web links, attachments & embedded media (video, images & audio)	Mandatory
The System is to enable Technicians to provide remote assistance to both Windows and Mac OS X devices or the API interface to allow another tool to do so	Mandatory
The System is to provide and comply with ITIL Management - Incident, Change, Problem, Release, Event and Request Fulfilment, including fully customisable Dashboards	Mandatory
The System is to provide Technicians with standard reporting and enable easy creation of customisable Reports	Mandatory
The System is to enable Managers to customise SLAs and KPI for Services and Customers	Mandatory
The System is to provide a customisable Customer satisfaction survey	Mandatory
The system should display a mandatory Hold reason when a ticket has been placed on hold as defined and customisable by Cabinet Office	Mandatory
Facility to enable attachments to tickets and tasks (media files, documents etc)	Mandatory
The System is to be able to Auto-generate tickets from emails in the Support mailbox based on customisable rules in both Google and MS O365 environments	Mandatory
The System should be able to prioritise, tickets raised for VIP or particular needs users	Mandatory
The System should be able to prioritise, Assets for VIP or particular needs users	Mandatory
Require ability to report on Agent Availability (logged on to take Calls/Tickets)	Mandatory
REST API which would provide access to asset (and other) data in a non-proprietary way using open standards.	Mandatory
Must be ISO/IEC 20000-1:2018, & MOF Compliant	Mandatory
Automated Resolution of Tickets based on Knowledge Base - Search of Articles to provide suggestions to Users	Mandatory
In App Live Chat and Call-Back functionality	Mandatory
Portal must have the ability to establish discrete Workspaces/Areas providing Full Functionality for Other Business Units to establish a dedicated URL link to their Area for users and discrete ticket management of these areas within the core Instance	Mandatory
Ability to control access to components of the tool with security groups	Important
The system should be able to manage multiple projects using industry standard tools such as Kanban, Scrum boards, epics, agile methodologies and stories.	Important
The System should be able to report on all aspects of the project lifecycle including aggregate time spent by project and individual	Important
Define a workflow on a project by project basis e.g. backlog/backlog/test/UX review/PO review	Important
The System is to enable Technicians to carry out Software audits	Important
The System is able to define and manage a Service catalogue so that it is searchable by Technicians and customers	Important
The system will provide Admins with customisable incident/request categories, closure codes, status and hold reasons for task/tickets/assets/users	Important

The System is to enable Customer or Technician to raise a ticket on behalf of another User	Important
The Customer portal should be able to be customised to our layout requirements	Important
The System is to provide the Customer with all assets and licence assigned to the Customer via the Customer Service Portal	Important
The System is to provide controlled access to a defined and managed Supplier and Contact list	Important
The System is to provide Ticket escalation control mechanism between resolver groups	Important
The System is to enable Technicians manage hardware Inventory	Important
The System is to enable KMS article approval and review mechanism	Important
The System is to provide Users with a live chat function via the Customer Portal. Integration with Beyond Trust's Cloud instance to facilitate Chat functionality and remote support	Important
The System to provide configurable SLA's and alert on any breach	Important
The system should send an automatic email to the Customer when a Ticket has been opened; suspended, released, resolved or closed.	Important
The ticket Hold reason must trigger customisable email actions as defined by Cabinet Office	Important
The system should be able to provide a client agent for asset activity and reporting, or the necessary API's for a tool to integrate with the system. Client record should provide Asset and Software information & include Software Licence End Dates. Asset Records to be editable to include Location Changes/Line Manager Changes etc.	Important
The System is to enable Managers to monitor and control device and licence Stock Levels	Important
The System is to enable Technicians to define and manage Software Licences	Important
The system should allow a method to highlight when an incident has been resolved via a "First Time Fix".	Important
All resolved tickets must be automatically closed after a customer satisfaction survey has been completed or manually closed by Technicians	Important
System should be able to perform some automated risk-management on proposed Changes based on asset/service affected.	Important
Automated Integration with 3rd Party Application for New Starters and Leavers to generate Starter/Leaver Ticketing, and identification of IT issues in systems such as SLACK	Important
Software Catalogue available to Users to request download - Auto Generate Approval Request if required & workflow to install	Important
Ability to archive/hide/remove redundant resolver groups without impacting historical data	Important
Ability to archive/hide/remove redundant incident/request categories, closure codes, status and hold reasons for task/tickets/assets/users without impacting historical data	Important
Function to deploy a automated chat system, to answer queries and log tickets via a conversational interface	Important
Function to integrate a number of AI/LLM-assisted functions to support agents in ticket management, such as writing replies, describing resolutions, and summarising tickets	Important

Function - enable the assistance of administration functions via a similar conversational interface as point 72, to assist with admin functions, app creation and coding, analytics insights and agent management	Important
Portal customisation manager - ability to make changes and customisations to customer portal with minimal coding requirements	Important

Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Platform pricing document) can't be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will include.

The Call-off Contract Charges shown in the below table details the cost breakdown for contract CO

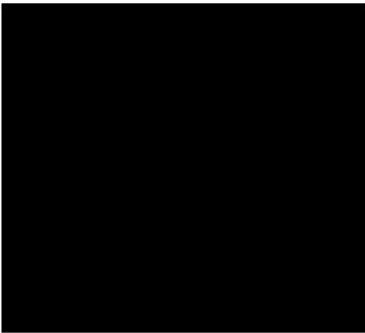
Total Net Price:	GBP 151,530
-------------------------	--------------------



TERMS	
This Service Order Form is governed by the Gcloud Call of Contract executed between Customer and Freshworks Inc. on [REDACTED] for the Services purchased from Freshworks (the "Agreement").	

Ver 3. Nov 28 2024 Freshworks Inc., 2950 S. Delaware Street, Suite 201, San Mateo, CA 94403

Freshworks Inc.		Customer	
Name	[REDACTED]	Name	[REDACTED]
Title	[REDACTED]	Title	[REDACTED]
Signature	[REDACTED]	Signature	[REDACTED]
Date	[REDACTED]	[REDACTED]	[REDACTED]



Schedule 3: Collaboration agreement- NOT USED

Schedule 4: Alternative clauses- NOT USED

1. Introduction

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

2. Clauses selected

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

2.1.1 Scots Law and Jurisdiction

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

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

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

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

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

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

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

2.3 Discrimination

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

Employment (Northern Ireland) Order 2002

Fair Employment and Treatment (Northern Ireland) Order 1998

Sex Discrimination (Northern Ireland) Order 1976 and 1988

Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003

Equal Pay Act (Northern Ireland) 1970

Disability Discrimination Act 1995

Race Relations (Northern Ireland) Order 1997

Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996

Employment Equality (Age) Regulations (Northern Ireland) 2006

Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000

Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002

The Disability Discrimination (Northern Ireland) Order 2006

The Employment Relations (Northern Ireland) Order 2004

Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006

Employment Relations (Northern Ireland) Order 2004
Work and Families (Northern Ireland) Order 2006

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

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

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

2.4 Equality policies and practices

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

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

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

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

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

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

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

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

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

2.5 Equality

2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

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

2.6 Health and safety

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

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

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

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

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

2.7 Criminal damage

- 2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Buyer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Buyer under any insurance policy).
- 2.7.2 If during the Call-Off Contract Term any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.
- 2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Buyer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Buyer's cost and the Supplier will (at no additional cost to the Buyer) provide any help the Buyer reasonably requires with the appeal.
- 2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

Schedule 5: Guarantee- NOT USED

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform).
Audit	An audit carried out under the incorporated Framework Agreement clauses.
Background IPRs	<p>For each Party, IPRs: owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes created by the Party independently of this Call-Off Contract, or</p> <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: 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: 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> <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	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-fortax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Financial Metrics	The following financial and accounting measures: Dun and Bradstreet score of 50 Operating Profit Margin of 2% Net Worth of 0 Quick Ratio of 0.7

Force Majeure	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any: acts, events or omissions beyond the reasonable control of the affected Party riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare acts of government, local government or Regulatory Bodies fire, flood or disaster and any failure or shortage of power or fuel industrial dispute affecting a third party for which a substitute third party isn't reasonably available</p> <p>The following do not constitute a Force Majeure event: any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans</p>
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.14 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.

G-Cloud Services	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.

Insolvency event	Can be: a voluntary arrangement a winding-up petition the appointment of a receiver or administrator an unresolved statutory demand a Schedule A1 moratorium a Supplier Trigger Event
Intellectual Property Rights or IPR	Intellectual Property Rights are: (a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information (b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction (c) all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: the supplier's own limited company a service or a personal service company a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or Buyer's possession before the Start date.
-----------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgement of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgement, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' Losses ' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement Schedule 6.
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.

New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
----------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------

Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Performance Indicators	The performance information required by the Buyer from the Supplier set out in the Order Form.
Personal Data	Takes the meaning given in the UK GDPR.
Personal Data Breach	Takes the meaning given in the UK GDPR.
Platform	The government marketplace where Services are available for Buyers to buy.
Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK GDPR.

Prohibited act	<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> <p>induce that person to perform improperly a relevant function or activity</p> <p>reward that person for improper performance of a relevant function or activity</p> <p>commit any offence:</p> <p>under the Bribery Act 2010</p> <p>under legislation creating offences concerning Fraud</p> <p>at common Law concerning Fraud</p> <p>committing or attempting or conspiring to commit Fraud</p>
-----------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to

	investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.

Services	The services ordered by the Buyer as set out in the Order Form.
Service Data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data and Performance Indicators data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.

Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controlscheck-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.

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

Term	The term of this Call-Off Contract as set out in the Order Form.
Trigger Event	The Supplier simultaneously fails to meet three or more Financial Metrics for a period of at least ten Working Days.
Variation	This has the meaning given to it in clause 32 (Variation process).
Variation Impact Assessment	<p>An assessment of the impact of a variation request by the Buyer completed in good faith, including:</p> <p>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>details of the cost of implementing the proposed variation;</p> <p>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>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.

Schedule 7: UK GDPR Information

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

Annex 1 - Processing Personal Data

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

- 1.1.1.1 The contact details of the Buyer's Data Protection Officer are: [REDACTED]
- 1.1.1.2 The contact details of the Supplier's Data Protection Officer are: [REDACTED]
- 1.1.1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.1.1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller and Processor for each Category of Personal Data	<p>The Buyer is Controller and the Supplier is Processor</p> <p>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:</p> <p><i>Personal data shall be used to provide the services.</i></p>
Duration of the Processing	Personal Data will be processed for the duration of the Call-Off Contract.
Nature and purposes of the Processing	The Personal Data processed will be subject to the processing activities required for providing the Services to the Customers per the Service Agreement.
Type of Personal Data	Name, email, nature of request, address, phone number, date of birth, security clearance
Categories of Data Subject	CO Staff

International transfers and legal gateway	<i>[Explain where geographically personal data may be stored or accessed from. Explain the legal gateway you are relying on to export the data e.g. adequacy decision, EU SCCs, UK IDTA. Annex any SCCs or IDTA to this contract]</i>
Plan for return and destruction of the data once the Processing is complete	<p>Controller may export all Service Data prior to the termination of the Buyer's Account. In any event, following the termination of the Buyer's Account</p> <ul style="list-style-type: none"> (i) Subject to (ii) and (iii) below and the Service Agreement, Service Data will be retained for a period of 14 days from such termination within which Controller may contact Processor to export Service Data; (ii) Where the Controller does not use custom mailbox and uses the e-mail feature, if available within the Service(s), e-mail forming part of Service Data are automatically archived for a period of 3 months; and (iii) logs are archived for a period of thirty (30) days in the log management systems, post which logs are retired to a restricted archived cold storage for a period of eleven (11) months (each a "Data Retention Period"). <p>Beyond each such Data Retention Period, Processor reserves the right to delete all Service Data in the normal course of operation except as necessary to comply with Processor's legal obligations, maintain accurate financial and other records, resolve disputes, and enforce its agreements.</p> <p>Service Data cannot be recovered once it is deleted.</p>

Annex 2 - Joint Controller Agreement- NOT USED

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

1.1.2.1 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.

1.1.2.2 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

1.1.3.1 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.

1.1.3.2 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

1.1.4.1 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.

1.1.4.2 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

1.1.5.1 The Parties shall:

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

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

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

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

1.1.7.1 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:

if in the view of the Information Commissioner, the Buyer is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Buyer, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Buyer, then the Buyer shall be responsible for the payment of such Financial Penalties. In this case, the Buyer will conduct an internal

audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Buyer and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

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

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

1.1.7.2 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.

1.1.7.3 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.

1.1.7.4 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

1.1.9.1 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: Service Definition Document

1. Introduction

Company Overview

Freshworks Inc. creates business software anyone can use. Modern, intuitive, and easily customizable for IT, customer support, and sales and marketing teams, our AI-boosted products are designed to let everyone work more efficiently and deliver more value for immediate business impact. Headquartered in San Mateo, California, Freshworks operates around the world to serve more than 67,000 customers, including American Express, Blue Nile, Bridgestone, Databricks, Fila, Klarna, OfficeMax and many others.

Business History

Girish Mathrubootham, the CEO of Freshworks (formerly Freshdesk), founded the company in 2010 with the aim of providing customer support software that departed from the traditional, clunky, and expensive interfaces. Since then, Freshworks has expanded its product offerings beyond customer service suite, with products covering IT service management, CRM (marketing automation and sales automation). Freshworks Inc. is now a publicly traded company (Nasdaq: FRSN). You can read more about our leadership structure here - <https://www.freshworks.com/company/leadership/>.

Locations

Headquartered in San Mateo, California, we have a dynamic team with approximately 4,900 employees operating from 13 global offices. Our reseller network comprises over 400 partners in more than 30 countries.

Our headquarters office is located in San Mateo, California, where we lease more than 20,000 square feet pursuant to a lease that expires in July 2026. We also maintain additional offices in the United States and internationally, including Denver, Seattle, our principal engineering facility in Chennai, India and other offices in London, The United Kingdom; Paris, France; Berlin, Germany; Utrecht, The Netherlands; Bangalore and Hyderabad, India; and Sydney and Melbourne, Australia.

Vision & Mission

Freshworks makes it fast and easy for businesses to delight customers and employees. Our Vision is to make our products and services fast and easily available for businesses of all sizes to delight their customers and employees across all touchpoints. Our Mission is to provide businesses with modern, unified, and intelligent SaaS products designed with the end user in mind. We do this by taking a fresh approach to building and delivering customer and employee engagement solutions that are quick to implement, easy to use, and affordable—enabling businesses to exceed customer and employee expectations to drive clear business results.

Product Portfolio

Freshworks is a leading provider of cloud-based Customer Support and Employee Engagement Suites that cater to an organization's support, sales, marketing, ITSM, and business teams.

We present the Freshworks Neo platform offering to deliver end-to-end platform design to unify customer experiences, enhance employee productivity, and empower an ecosystem of developers and partners. Imagine the simplicity and efficiency of having a single platform to customize, integrate, and automate workflows for customer support, IT, and CRM use cases

Listen to our customer testimonials explaining why they are delighted with us here.

Value Proposition

There are many reasons our clients choose us and retain us (99% enterprise customer retention rate). Some of the top reasons are:

Ease of Use: Our products are designed with care and loved by users (G2Crowd and Gartner Peer Insights), ensuring user acceptance and enthusiastic adoption.

Platform: Our scalable platform anchors a seamless cross-product experience that offers 360° customer coverage to enable your service strategy. Open APIs allow in-product customization and over 700+ readily available 3rd-party integrations.

Innovation: Our thought leadership on how customer engagement should be run to create memorable customer experiences fuel our innovative product roadmap that tries to stay ahead of trends across various engagement channels, automation, bots, etcetera.

Empowering through AI: Freshworks' AI, fondly known as "Freddy," helps sales, marketing, and support professionals with predictive insights across the customer journey. With Freddy AI, we build and refine our Machine Learning models to unlock our customer data value. To make the power of AI accessible, Freddy is always learning new skills, surfacing predictive insights, automating repetitive tasks, and pointing out new opportunities so you can focus on building customers-for-life.

Partnership: Our long-term focus forces us to look beyond the generic "vendor relationship" common in the market today. We provide our customers with every resource they need to ensure that they are successful without the expensive professional services fees. We provide highly-present resources who listen, engage, and deliver your desired solution together as one team.

Value: Our products are designed for speedy implementation, rapid agent adoption, and consequently, quicker time to value. Coupled with our industry-leading no-surprise pricing, we offer the best value in the market today.

Security: We take the utmost care in the processing and storing of your client's data. We host our European client's data with AWS. We comply with significant data security and data privacy regulations, including GDPR, and have secured many certifications.

What the Service Provides

Freshservice is a SaaS based IT Service Management product from Freshworks and was launched in the year 2014. Freshservice is a cloud-based ITSM software for your service desk with powerful automation tools to manage Incidents, Problems, Changes, Assets, and more. The platform empowers your team to modernize ITSM with an intuitive, quick, time-to-value solution.

We at Freshworks offer a platform where you have

Robust Automation through which you can eliminate repetitive tasks and manual processes and drive service efficiency using no-code workflows and powerful automation

An Integrated Platform through which you can integrate service management on a single platform to bridge silos, improve time to resolution, reduce costs, and improve visibility

Rapid Deployment, where you can customize rapidly with Freshservice's no-code platform. Get expert onboarding, migration services, and 24x7 support.

Freshservice, since its inception, has been going through constant enhancements through minor and major releases. All the rollouts are planned and communicated to customers well in advance through identified channels. Freshservice, being a Software-as-a-Service (SaaS) based product, does not have different versions of the product but has different plans to choose from depending on your requirements.

Overview of the G-Cloud Service

Freshservice is the award-winning ITSM product by Freshworks, a global, multi-product company with over 150,000 business customers globally. At Freshservice, our objective is to modernize IT and other business functions with a refreshingly easy-to-use, simple-to-configure IT service desk solution. It is a cloud-based platform used to manage an organization's IT incidents and enterprise-wide service requests. IT Managers and Admins can use Freshservice to provide the best support possible to their end-users.

Freshservice is a cloud-based Software-as-a-Service (SaaS) IT Service Management solution that follows the ITIL guidelines and best practices with simple, refreshing and intuitive user experience, bringing ITIL processes like Incident, Service Request, Problem, Project, Change and Release

management right into one Service Desk. All of these processes revolve around IT assets which are provided in a robust CMDB to manage your Configuration Items (CIs). Freshservice also lets you publish your solution articles to the knowledge base hosted on the cloud. Freshservice strives to keep IT support fun, with its gamification system to keep support agents motivated and productive. As a product, Freshservice has been developed leveraging Freshworks' experience in providing user-friendly, omnichannel support solutions. Freshservice has everything you need for your IT support needs:

Easy to Access, Use, and Configure: Modern and intuitive UI requires minimal to no training and is customizable to IT and non-IT needs. The administration of Freshservice is undertaken via a graphical console and requires no coding. All are delivered from the cloud. Accessed from a web browser at any internet-enabled location.

Multi-channel Support: Automate tasks and support issues raised via email, self-service portal, phone, chat, or in person.

Information at Your Fingertips: Maintain records of contracts, hardware, software, and other assets, including all details from acquisition to expiry

Best-Rated Mobile App: Leverage the best-rated mobile service desk app for iOS and Android and support your high-impact employees who are on the road

Best in Implementation: Freshworks has great experience implementing solutions globally.

Here are some of the benefits that come along with using the Freshservice ITSM module –

Align your IT infrastructure to ITIL processes:

Equip your service management platform with the industry standards set by ITIL to quickly respond to changes, improve reliability, and proactively predict and prevent issues, thus setting up a high-velocity service delivery process.

Empower end-users with consumer-grade experiences:

Retain focus on end-users by communicating with them on the channel of your choice, offering them access to an enriched knowledge base and enhanced self-service experience, to access all IT services through a unified service catalog.

Make informed decisions with analytics:

Analytics for decision-making and continual improvement in the IT department by decreasing the levels of uncertainty. Track and assess both faculty performance and service desk metrics holistically with analytics, build reports from scratch, and get quick insights using curated reports.

Increase faculty efficiency:

Create contextual and intelligent experiences through AI to improve process efficiency and service agility. All the means to ensure your end-users receive the best customer experience. Enable agents with ML-powered suggestions and responses, and put time back into their day so they can focus on more strategic initiatives.

As a trusted partner, Freshworks will always deal with your requirements directly throughout the sales and customer lifecycle. We are committed to your success, and you will have direct access to our technical resources and insight into our product roadmap.

This approach has resulted in Freshworks being awarded the Service Desk Institute's award for best ITSM Implementation two years in a row (with Western Sussex in 2017 and Descartes in 2018). We will provide a fully managed implementation and will not surprise you with extra costs for

implementation and upgrades, nor will you have to maintain increasingly expensive product experts internally or purchase professional services at considerable expense from resellers. Freshworks has a huge developer base, which enables us to be very agile and responsive in addressing customer requirements and creating innovative solutions.

Associated Services

Maintenance & Support: Freshworks owns the complete application support and maintenance for the customer's Freshservice instance. This includes 24x7 technical support to troubleshoot any issue the customer may face or to answer any customer query. Customers will also be provided with a Technical Account Manager who will be a single point of contact with complete context on the customer's configuration settings and use cases (as shared by the customer).

Freshworks also has an active Network Operations Team that monitors the network traffic to Freshservice accounts globally.

Professional Services: Freshworks will employ a dedicated Technical Account Manager (TAM) to help in pre-implementation assessments, requirement discovery, and implementation and training. An Engagement Manager (EM) will be available to coordinate the complete onboarding journey. All the project management activities will be taken care of by the EM.

Our customer success team provides post-implementation support. TAM and EM will be part of the initial Hyper care period until our Customer Success Manager (CSM) understands the customer environment. Freshworks customer success team will engage with customers to enable product adoption. A dedicated CSM and support team will engage with the customer to provide any post-implementation support. The CSM will also ensure you get the most out of your Freshservice instance. This will include conducting Quarterly Business Review (QBR) meetings, objective setting, annual reviews, and proactive feature meetings when new or relevant features are released.

API: Freshworks provides public documentation of our developer SDKs as well as APIs. Using our powerful, open APIs and SDK capabilities, Freshservice can integrate with a variety of external, third party systems and solutions. Freshservice's APIs belong to the REpresentational State Transfer (REST) category. This means that they can be used to perform "RESTful" operations such as reading, modifying, adding or deleting data from a service desk. The below links take you to our A-Z developer guide and our comprehensive list of API endpoints, respectively:

<https://api.freshservice.com/v2/>

2. Data Protection

Information Assurance

Freshworks' security & privacy policies and controls, being a multi-tenant SaaS provider, complies with standards and guidelines applicable to our services. Freshworks process and controls comply with the below standards as of today

ISO 27001 - Audited & Certified by an independent third party

ISO 27701 - Audited & Certified by an independent third party

SOC II - Audited & Attested by an independent third party

GDPR -Product features, technical and organizational measures audited above and DPAs

Cyber Essentials & Cyber Essentials Plus - Audited & Certified by a third party

Refer to www.freshworks.com/security for more details. Freshworks security documents/reports can be requested from the following link: <https://trust.freshworks.com/>

Data Back-Up and Restoration

Freshworks backs up data in the following ways.

A continuous backup is maintained in another AWS data center (i.e., AWS Availability Zones) within the same region, which is at least 100 km apart.

Cloud Snapshots(Incremental backups) are taken daily and retained for the last seven days.

Backup Data is encrypted at rest using industry-standard AES 256-bit encryption as the original data and is stored in the same region as the primary Data centre.

Freshworks uses AWS RDS, which is a managed service, for the database. AWS RDS provides automated backups, which are immutable, with a lifecycle policy that ensures deletion doesn't happen. Except for the SRE team (warranted based on their job responsibilities following the least privilege and need-to-know basis), no one else from Freshworks can access the database.

Individual customers cannot define their own backup terms as these are configured at an infrastructure level.

Backups are managed using a Shared Responsibility Model between Freshworks and AWS. AWS is responsible for scheduling backups, performing backup restoration tests, and ensuring the integrity and availability of backups. Freshworks will specify which system/ data to back up, the frequency of backup, the type of backup, which backup to restore, and when.

On a yearly basis, a Disaster Recovery test is performed for each application, where the backup is restored and tested for its integrity.

Business continuity statement/plan

Freshworks has a formal Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) defined and implemented to enable people and process support during crises or business interruptions. Appropriate roles and responsibilities have been defined and documented in the BC plan. Freshworks Information Security Office and respective Customer Manager will be responsible for communication and notification during a crisis.

The BCP and DR Plan is tested and reviewed annually by the Freshworks Information Security Officer and approved by the CPSC (CyberSecurity and Privacy Steering Committee). BCP and DRP requirements training is provided to all relevant employees involved in the process every year. The BCP and DR plan of Freshworks is reviewed and audited as part of ISO 27001 standards and SOC 2 Type II, covering availability as one of the trust service principles.

The BC-DR for Cloud Services document, Freshworks BC-DR Plan document, and BC-DR Executive summary can be requested using the following link - <https://trust.freshworks.com/>.

Privacy by Design

Freshworks is committed to providing secure products and services by implementing and adhering to requirements under GDPR, both as a data controller and processor. Freshworks is ISO 27701 certified and has a comprehensive GDPR program headed by the legal team with assistance from the information security team. Key privacy principles supported are - Accountability, Privacy by Design and Default, Data Minimization, and Subject Access Rights.

Programs, projects, and processes at Freshworks are aligned to GDPR Privacy Principles right from the inception of an idea or project, thereby supporting Privacy by Design and Default principles.

Freshworks' privacy practices, both as a controller and a processor, can be found at <https://www.Freshworks.com/privacy/>.

As a processor, Freshworks offers a data processing addendum to its customers (controllers) at <https://www.Freshworks.com/data-processing-addendum/> as part of the sign-up terms and conditions.

Further, customers are encouraged to refer to the following pages:

Security Policy - <https://www.freshworks.com/security/>

Sub-Processors - <https://www.freshworks.com/privacy/sub-processor/>

Data Hosting pages - <https://www.freshworks.com/privacy/data-hosting/> Freshworks has completed the following as part of the GDPR implementation:

Data privacy impact assessment while employing new technologies

Maintaining Data Processing Records

Sub-processor due diligence

Privacy-by-design with product features that also enable our customers to comply with their obligations under GDPR

Monitoring and governance process

Periodic reviews of policies and procedures applicable to data protection

Companywide mandatory training and privacy playbooks for certain functions (i.e., Product development and HR)

3. Using the service

Ordering and Invoicing

To order or discuss any Freshworks services, please email one of the dedicated members of the Freshworks team below to discuss your requirements or place an order.

fredrik.hallberg@freshworks.com - Fredrik Hallberg, Regional Director - Sales (Education)

nick.daley@freshworks.com - Nick Daley, Regional Director - Sales (NHS, Central Government, Local Government)

Availability of Trial Service

Freshworks offer a 14-day fully-functional free trial of the Freshservice platform on any plan. Our product experts guide you through your evaluation, also free-of-charge. After the given evaluation period, you can then select a plan to continue using the product. Link to signup

<https://www.freshworks.com/freshservice/signup>.

On-Boarding, Off-Boarding, Service Migration, Scope etc.

Freshworks can support [ClientName] migration from your existing platform to Freshservice. The platform can facilitate the migration of tickets, notes, solution articles, agents, groups and more. The Onboarding phase has a dedicated Onboarding Specialist, and Engagement Manager will be assigned for [ClientName]. The dedicated point of contact will work with [ClientName] and help facilitate a successful onboarding process.

Training is often the key to adoption, so we will train the majority of Agents and Admins of Freshservice. These training sessions are a part of the overall package and there are no additional costs associated with them.

Best Practices for onboarding and adoption:

Training and documentation: We will be conducting comprehensive training sessions for administrators, agents, and end users, and each of these sessions will emphasize the best practices to be followed, thus enhancing their efficiency and effectiveness while also boosting adoption. The accompanying documentation will also help them become well-versed with these best practices.

Post-implementation support: Freshservice will employ a dedicated Technical Account Manager (TAM) and a Customer Success Manager (CSM) for the account. The CSM will engage with you to increase product adoption, promote best practices, and to ensure you get the most out of your Freshservice instance. This includes conducting Quarterly Business Review (QBR) meetings, objective setting, annual reviews, and proactive feature meetings when new or relevant features are released. The Customer Success team at Freshworks thrives on nurturing a long-term relationship beginning with a successful onboarding.

The project's assigned Customer Success Manager (CSM) will be involved with the project during the hypercare phase. A handover in terms of process and configurations knowledge transfer will be done. The two weeks of hypercare will have the implementation team and the

CSM involved in a warm transfer. After the hypercare period, the CSM will remain the single point of contact. We will also identify a Technical Account Manager for product go-to and have our 24*7 support team available for any day-to-day transactional questions email, and 24*5 support team on chat and phone.

Documentation: Our training program will be accompanied by full-fledged product documentation. You will also be able to access online documentation and solution articles at this link:

<https://support.freshservice.com/support/home>. The documentation also consists of easy-to-understand online tutorial videos to help you use Freshservice better.

Upon termination or expiration of this Agreement or any SOF for any reason, Customer's access to the Services, Software, Mobile Apps, APIs, and other Freshworks Technology will terminate. Freshworks strongly recommends that Customer export all Customer Data before Customer closes Customer's Account. Freshworks will make Customer Data available for export for fourteen (14) days from the effective date of the closure of Customer's Account due to: (i) the termination or expiration of this Agreement, or (ii) termination or expiration the applicable SOF ("Data Export Period"). Where Customer Data is retained by Freshworks and can be exported, and provided that Customer is current on its payment obligations as described in Section 5, Customer may contact Freshworks within the Data Export Period at support@freshworks.com to have Freshworks export Customer's Customer Data. Beyond such Data Export Period, Freshworks reserves the right to retain Customer data for up to three (3) months before deleting all Customer Data in the normal course of operation except as necessary to comply with Freshworks legal obligations, maintain accurate financial and other records, resolve disputes, and enforce its agreements. Customer Data cannot be recovered once it is deleted.

Training

During the implementation, Freshworks will conduct demos of the configurations to demonstrate implemented functionality. These demos serve as a vehicle to ensure Freshworks is delivered per requirements and correct the implementation where requirements are unmet. Once the configuration of the Freshworks product is complete, User Acceptance Testing (UAT) will be performed. Project plans are shared with the customer and/or the customer's project manager to share and agree on the project's status, including the testing phase. After assessing the training needs of the [ClientName], The Freshworks implementation team will develop a training plan. Freshworks believes training is a key factor in increasing the tool's adoption. Training will be customised based on the [ClientName]'s portal (post-product implementation). All supporting materials and training resources will be available in the package.

Apart from the in-product first-time experience suggestion like setting up the support channels and navigating within the tool, we have abundant training resources available online to ensure our customers get the help needed throughout their journey with Freshworks, right from setting up the tool to being able to excel in managing the tool. Freshworks Academy has training materials for all types of stakeholders using the tool (Agents and Admins). Our customers can also use additional support like video tutorials and Knowledge-based solution articles to get the required solution. We also have an active community forum to enable our customers to interact with other customers and our product team on any feature request, Ideas, or Issues that our

product team reviews and provides updates/solutions. Freshworks will confirm the go-live readiness and do a project wrap-up hand-off with the relevant stakeholders on your side.

Implementation Plan

A detailed implementation plan can be provided to the buyer on request.

Service Management

Maintenance Window: Freshservice product features are pushed out as and when they become available. This is done once every month at present, but this may vary if the speed of releases is changed. These releases are designed to minimize the impact as the live production instance of Freshservice is switched to a failover instance. Then, once the upgrade/ patch is loaded, tested, and certified to be stable, the live model is changed back to production. As such, these upgrades have no impact on the end-user, and they can continue carrying out their usual day- to-day activities on Freshservice. This highly resilient infrastructure has resulted in 99.8% availability.

Regarding product upgrades, releases are as often as every week. However, most of these releases are undertaken with no functional changes to Freshservice and are primarily security patches and platform improvements. We follow the blue-green deployment strategy for deploying changes to the production environment, allowing us to introduce new changes without downtime and roll back without impacting any existing users. Typically, we do not require rest for routine deployment of enhancements.

Customization: The Freshworks team will work with [ClientName] to support you with the initial set-up and configurations on the platform. In the course of the implementation, the [ClientName] ITSM team will be extensively trained on the Freshservice platform with regards to the customizations as well.

Post-implementation, the [ClientName] team will be equipped to configure the platform independently and can leverage the training material and the abundantly available video tutorials/solution articles to carry out any customizations needed.

Freshworks also offers a dedicated technical account manager (TAM) and a customer success manager(CSM) who you can reach out to at any given point to help with any assistance. The TAM and CSM are assigned to help you make the best out of your Freshservice instance.

Freshservice operates on a structured schedule for the deprecation of features, with two designated periods in May and November. It's worth noting that such occurrences are rare. However, in the event of a deprecation, we are committed to ensuring our customers are well- informed. As such, we will provide all our customers with a six-month advance notice regarding any changes, along with any necessary actions that may be required on their part.

Service Constraints

We provide a platform availability of 99.8%. Current and historical availability information can be seen here: <http://status.freshservice.com/>

Freshworks provides standard quality support to all its customers and there are no additional charges involved for support. Freshservice support team works 24*7 and you can reach out to Freshservice technical support team over Email (24x7), Phone (24x5), Chat (24x5), and Portal

(24x7); all contact coordinates for support are available at our Support Website

<https://support.freshservice.com/en/support/home>.

Freshservice will provide ongoing support and maintenance for all the elements of the Freshservice instance. This includes 24x7 technical support to troubleshoot any issue the customer may face or to answer any customer query. This means Freshservice will provide first level (L1) through fourth level (L4) support. We will also assign a Technical Account Manager (TAM) who will act as a single point of contact and will be able to handle the support queries from you. Reachability hours can be mutually discussed and agreed upon.

Service Levels

Across all products and services, Freshworks provides an uptime of 99.8% per calendar month. This translates to roughly 20 minutes of allowed unplanned downtime in any given week or 1hr 29m 39sec of downtime in a month.

Support Availability: Freshworks will provide 24/5 telephonic and chat support and 24/7 email support

Support Response Timelines: Depending on the severity of the issue, Freshworks' response times range between 2 hours to 8 hours.

Issue Resolution Timelines: Per policy, Freshworks does not commit to any defined resolution timelines in our SLA Agreement.

The detailed SLA document will be shared with the prospect later in the discussion.

Outage and Maintenance Management

Freshworks owns the complete application support and maintenance for customer's Freshservice instance. This includes 24x7 technical support to troubleshoot any issue the customer may face or to answer any customer query. Freshworks also has an active Network Operations Team that monitors the network traffic to Freshservice accounts globally.

The frequency of new feature releases is once a month, and enhancements to released features and bug fixes can roll out daily. There is no scheduled time during the day when releases are made and fixes are performed. Since Freshworks products are cloud-based and built on a highly resilient architecture, there is no impact on the administrators, agents and customers when code is updated. Any new release or upgrade will not disrupt the existing configurations in the system. The existing customizations will be carried to the latest version by default.

Freshservice will provide you with a sandbox or a testing instance/environment to perform all the testing before rolling out anything to the production instance. With Sandbox, you can create an out-of-the-box environment to test out workflows and configurations before syncing them to your Freshservice account (a.k.a your production account) while keeping away from ramifications. Though Sandbox mirrors your Freshservice account, tickets, customer data, and contact information will not be copied.

Financial Recompense Model for not Meeting Service Levels

A detailed SLA document will be shared with the prospect later in the discussion.

4. Provision of the service

Customer Responsibilities

No additional requirements or responsibilities on the customer outside of the standard agreement.

Technical Requirements and Client-Side Requirements

We recommend users of the Freshworks platform check with their system administrators to ensure the following system and browsers are available.

Operating System Requirements

Ensure that your computers have one of the following operating systems installed:

Windows 7.0 or Higher

OSX Mavericks or Higher

We recommend referring to Microsoft or Apple websites on their minimum hardware requirements for the operating system to run smoothly.

Browser Requirements

Chrome/Firefox/Safari/Edge: Latest 2 versions

Browser Feature Requirements

Depending on the browser of your choice, you will then have to configure the following browser features:

JavaScript must be enabled.

Cookies must be enabled.

LocalStorage must be enabled.

HTTPS - TLS v1.2 or Higher. Previous versions have been deprecated.

Customer Team Roles

Project Manager

Day-to-day relationship management, project management and escalations for the customer. Engages on-demand resources to drive project success.

Conduct weekly meetings with key stakeholders and provide weekly updates to executive management to ensure project progress.

Technical Lead

Knows and understands the technical landscape of the customer, has access to people/systems to allow integration, migration, and testing of tools.

Responsible for technical decisions and customer side setup (e.g. setup SSO or help desk

Business Owner

Strong understanding of the customer's business processes, across departments, strategy, business goals, and metrics necessary for the project

POC for decisions on workflows, team collaboration, reporting, etc. Can be the PM, if above is given

System Administrator

Configures and maintains the tool with the help of Freshworks Product Specialist

Will help to prepare and execute training of customer agent.

Development life cycle of the solution

We use an Agile-aligned methodology for delivery which also takes in some best practices for project management from the waterfall delivery model. This approach helps us manage risks and deliver on time and budget. Additionally, for any software development required in terms of custom app development or 3rd party integrations, we use the Agile-influenced methodology for the onboarding process. We deliver the scope of the project in two-week sprint cycles. A tentative sprint outline is prepared to help gauge the timeline (and the total number of sprints) to complete the onboarding effort. This methodology allows us to focus on the features and requirements most critical to the business and deliver a working and thoroughly tested Freshworks solution.

The implementation will involve scoping, meetings with your team to finalize the plan, configuration, customization, migration, Testing, Training and finally, go live. Below are the phases in which the implementation is done.

Initiate: This phase aims to set a strong foundation for a successful go-live with no risks. Major outcomes of this phase are gathering all requirements, defining scope and objectives, outlining key project activities along with roles and responsibilities, and training your system administrators and product champions on the configuration process.

Configure: All the configurations and integration requirements are addressed and implemented. We will assist you with the set-up and integration of Freshworks Marketplace apps with your CES or EES instance. Marketplace offers a wide selection of apps that can be configured in a matter of minutes.

Data Migration: Freshworks can support migration from your existing platform to the Freshworks solution. The platform can facilitate the migration of tickets, notes, solution articles, agents, groups, and more. You can have a glimpse at the migration plan proposed by Freshworks below.

Test and Train: At this stage, the Freshworks onboarding team will work with [ClientName] to create test cases, agree on the test timeline, and coordinate to complete the testing on time. Freshworks follows the train-the-trainer model for product champions who will, in turn, train support teams and departments.

Hypercare: Once the project goes live, the engagement manager and onboarding specialist will work with you on platform adoption maximization, configuration optimisation, and product support.

After-sales Account Management

At Freshworks, we understand that your business's evolving needs require us to continuously provide the right level of support and ongoing stakeholder alignment. The Customer Success team at Freshworks is your guide to navigating the post-sale journey with you. Our team of Customer Success Managers (CSMs) focuses on ensuring our customers successfully deliver their business outcomes from their investment. By using proven methodologies to support the joint development and execution of a Success Plan, your CSM ensures the Customer Success Plan provides the foundation, visibility, and tracking of identified Key Performance Indicators (KPIs). Your customer success plan will map your business benefits to the software investment you've made.

Your CSM will ensure access to the Freshworks ecosystem – senior management product management, product roadmaps, engineering access, and support from the business units, as required. CSMs at Freshworks want to help simplify the complexity of your world, build on the implementation, drive software adoption, and look for business benefits aligned with your strategy to exploit the full capability of your investment and measure KPIs that align with identified value. To ensure you realize value from your investment, we work with you to drive transformation across your business, delivering ROI reporting and ensuring that your satisfaction with Freshworks improves (as measured by NPS). We use our proven tool kit, which introduces access to industry best practices, tracking the adoption of your software and linking to specific KPIs.

Your CSM resources are seasoned industry leaders with IT and Customer Service portfolio expertise. We operate as a value champion for your business, ensuring customer advocacy into Freshworks. We do this by providing a senior trusted advisor as a single point of contact, incentivised by your success, with access to the Freshworks ecosystem to drive the joint development of the success plan and governance. Our CSMs are experienced people: experienced in Freshworks but also in the wider business world. Our role is not to sell you software – we are not a technical resource – our role is to understand and value the challenges and work with you on the cases, tied to business benefit, mapped to a measurable value.

We understand that our customers invest in our products and services because you want to use them to help achieve a set of positive outcomes: Customer Success is all about helping you to do just that. It's about being clear on the outcomes you want to achieve and understanding what needs to be done in order to achieve them. It's about putting mechanisms in place to track progress and identify as early as possible when corrective action is needed and it's about accountability: holding your people accountable for staying the course – ensuring value

realization and benefits management is part of the normal operating model and culture and holding Freshworks accountable for its part of the bargain.

Termination Process

Please refer to <https://www.freshworks.com/terms/>

Our experience

Case Studies

Suffolk County council

University of Aberdeen

Citizens Advice

Clients

<https://www.freshworks.com/customers/>

Contact Details

For any other questions relating to Freshworks and the G-Cloud listing, please reach out to any of the dedicated Freshworks representatives below.



Schedule 9 (Corporate Resolution Planning)

Definitions

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</p>

	British Pound Sterling at the closing exchange rate on the Accounting Reference Date;
“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> <p>any change of Control of the Supplier or a Parent Undertaking of the Supplier;</p> <p>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;</p> <p>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;</p> <p>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;</p> <p>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;</p> <p>payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the Net Asset Value of</p>

	<p>the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any 12 month period;</p> <p>an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group;</p> <p>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;</p> <p>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</p> <p>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;</p>
"Corporate Change Event Grace Period"	<p>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;</p>
"Corporate Resolvability Assessment (Structural Review)"	<p>means part of the CRP Information relating to the Supplier Group to be provided by the Supplier in</p>

	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”	<p>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;</p>
<p>“FDE Group”</p> <p>“Financial Distress Event”</p>	<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;

Service Status and Supplier Status

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

Schedule 10 - Variation Form

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

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

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

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

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

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

Signature

Date

Name (in Capitals)

Address

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

Signature

Date

Name (in Capitals)

Address