Crown Commercial Service

G-Cloud 13 Call-Off Contract

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

G-Cloud 13 Call-Off Contract

Part A: Order Form

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	MongoDB Atlas Enterprise Package 9591 1102 5794 492 (the "**MongoDB Atlas Enterprise Package**") MongoDB: Consulting 5520 2729 2439 363 Training: Private Training Class per Day 9444 1361 2840 759 (together, the "**Professional Services**") Named Technical Services Engineer 5450 1327 4476 968 (the "**NTSE Services**")
Call-Off Contract reference	MongoDB Reference: Q-150692; DWP Reference: ecm_11605

Call-Off Contract title	MongoDB Atlas Enterprise Package MongoDB: Consulting Training: Private Training Class per Day Named Technical Services Engineer
Call-Off Contract description	MongoDB: Consulting Training: Private Training Class per Day MongoDB Atlas Enterprise Package Named Technical Services Engineer – should an ongoing need be identified after March 2024 and subject to a contract variation signed by both parties.
Start date	February 1, 2024
Expiry date	January 31, 2027
Call-Off Contract value	The value of the Buyer's estimated spend under this Call-Off Contract is £21,952,950,000. To the extent that the Buyer's use of the Services exceeds such value, the Buyer shall be liable to the Supplier for such additional sums.
Charging method	Monthly in arrears for consumption for MongoDB Atlas Enterprise Package Redacted: FOI SECTION 43 COMMERCIAL INFORMATION Redacted: FOI SECTION 43 COMMERCIAL INFORMATION

Purchase order number	To be provided by the Buyer, post Call-Off contract signature.

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

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

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

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

From the Buyer	Department for Work and Pensions 2 St Peters Square Manchester M2 3AA United Kingdom

To the Supplier	MongoDB Limited Building 2, Number 1 Ballsbridge Avenue, Shelbourne Road, Dublin 4 D04 Y3X9 Ireland Company number: 499992
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: Redacted: FOI SECTION 40 PERSONAL INFORMATION
Name: Redacted: FOI SECTION 40 PERSONAL INFORMATION

Email: Redacted: FOI SECTION 40 PERSONAL INFORMATION
Phone: Redacted: FOI SECTION 40 PERSONAL INFORMATION

For the Supplier:

Title: Redacted: FOI SECTION 40 PERSONAL INFORMATION
Name: Redacted: FOI SECTION 40 PERSONAL INFORMATION

Email: Redacted: FOI SECTION 40 PERSONAL INFORMATION
Phone: Redacted: FOI SECTION 40 PERSONAL INFORMATION

Call-Off Contract term

Start date	This Call-Off Contract Starts on February 1 , 2024 and is valid for **36 months, until 31th January 2027.**
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least **90** Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause (as per clause 18.1). Notwithstanding any other provision of this Call-Off Contract, in the event that the Buyer exercises its rights under Clause 18.1 of this Call-Off Contract the Buyer shall remain responsible for (1) all fees incurred in relation to this Call-Off Contract for all of the MongoDB Atlas Enterprise Package consumed up to and including the end date in the termination notice and (2) all fees set forth on this Call Off Contract for the Professional Services, and Buyer shall not be entitled to any refund in respect of prepaid fees for unused subscriptions.

Extension period	The MongoDB Atlas Enterprise Package (Platform Service ID Number - 9591 1102 5794 492) subscription purchased in this Call Off Contract can be renewed by the Buyer for 1 period of 12 months, by giving the Supplier 30 days written notice before its expiry. The renewal periods are subject to clauses 1.3 and 1.4 in Part B below and must follow the Variation Process defined in clause 32 in Part B The Buyer may renew the MongoDB Atlas Enterprise Package (Platform Service ID Number - 9591 1102 5794 492) subscription purchased in this Call Off Contract for one additional annual (12 month) term at the price set forth in this Call Off Contract, as long as the renewal quantities remain at least the same and the subscription term is continuous with the MongoDB Atlas Enterprise Package (Platform Service ID Number - 9591 1102 5794 492) subscription in this Call Off Contract.

Buyer contractual details

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

G-Cloud Lot	This Call-Off Contract is for the provision of Services Under: ● Lot 2: Cloud software ● Lot 3: Cloud support
G-Cloud Services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below: **MongoDB Atlas Enterprise Package** Service ID 959111025794492

	https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/959111025794492 **MongoDB: Consulting** Service ID 5520 2729 2439 363 https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/552027292439363 **Training: Private Training Class per Day** Service ID 9444 1361 2840 759 https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/944413612840759
Additional Services	N/A
Location	The Services will be delivered by the Supplier to the Buyer remotely.
Quality Standards	N/A
Technical Standards:	The technical standards used as a requirement for this Call-Off Contract are: Technical And Organizational Security Measures | MongoDB (https://www.mongodb.com/technical-and-organizational-security-measures) and attached as Exhibit A to this Call Off Contract (the "**Technical Standards**"). The Supplier may modify the Technical Standards from time to time, but the Supplier will not do so in a way that materially and adversely affects the overall security of the Cloud Services. The Supplier will notify the Buyer of any changes to the Technical Standards by emailing the address associated with your account.
Service level agreement:	The service level and availability criteria required for

	this Call-Off Contract are: MongoDB Atlas Service Level Agreement | MongoDB https://www.mongodb.com/cloud/atlas/sla The current version of the SLA for MongoDB Atlas is attached as Exhibit B. While the Supplier may modify the SLA from time to time, the Supplier will provide the Buyer with 90 days' notice regarding any adverse changes to the SLA by emailing the address associated with your account.
Onboarding	N/A

Offboarding	N/A
Collaboration agreement	N/A

Limit on Parties' liability	Notwithstanding Section 24 of Part B: Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed twice the fees payable by the Buyer to the Supplier during the Call-Off Contract Term. The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data will not exceed **100%** of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term. The annual total liability of the Supplier for all other Defaults will not exceed **100%** of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.
Insurance	The Supplier insurance(s) required will be: ● a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract ● professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law); and ● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law.

Buyer's responsibilities	N/A
Buyer's equipment	N/A.

Supplier's information

Subcontractors or partners	The Supplier may engage qualified subcontractors to provide the Consulting Services, and the Supplier is responsible for any subcontractor's compliance with this Agreement.

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 (Bankers Automated Clearance Service).

Payment profile	The payment profile for this Call-Off Contract is: ● Monthly in arrears for consumption for MongoDB Atlas Enterprise Package at the unit price set forth in this Call-Off Contract. ● Professional Services – Fixed Price Upfront Payment. Please refer to “Charging Method” above for a full breakdown. Subscriptions are non-refundable and non-cancellable except as set forth in this Call-Off Contract and expire at the end of each subscription period.
Invoice details	The Supplier will issue electronic invoices monthly in arrears for consumption. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice. The Supplier will issue an electronic invoice for the price, one off, Professional Services. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice. Please refer to “Charging Method” above for a full breakdown.
Who and where to send invoices to	Electronic Invoices (attached to E-Mails) should be sent to: Redacted: FOI SECTION 40 PERSONAL INFORMATION Paper invoices should be sent to: Department of Work and Pensions SSCL, PO Box 406, Phoenix House, Celtic Springs, Newport

	NP10 8FZ A copy should also be emailed to: invoicing.technologycsmt@dwp.gov.uk
Invoice information required	All invoices must include: · Valid purchase order number; · All files/invoices must be in PDF format; · One PDF per invoice – all supporting · documentation must be included within the · single PDF; · Supplier should not attach additional/separate supporting documentation as a separate file. Multiple invoices can be attached to one email but each invoice must be in a separate PDF (with no additional supporting files as described above).
Invoice frequency	Invoice will be sent to the Buyer in line with the payment profile and charging method.
Call-Off Contract value	The value of the Buyer's estimated spend under this Call-Off Contract is £21,952,950,000. To the extent that the Buyer's use of the Services exceeds such value, the Buyer shall be liable to the Supplier for such additional sums.

Call-Off Contract charges	The breakdown of the Charges is detailed in **Schedule 2.** All charges exclude applicable taxes and are due Net 30 days from the invoice date.

Additional Buyer terms

Performance of the Service	N/A
Guarantee	This Call-Off Contract is covered by the Parent Company Guarantee agreed in Call-Off Schedule 5. As per clause 4.10 in the Framework Agreement, if requested by a Buyer, the Supplier must provide a completed Guarantee before the Call-Off Start date in the form set out in Call-Off Schedule 5
Warranties, representations	N/A
Supplemental requirements in addition to the Call-Off terms	N/A

Alternative clauses	N/A
Buyer specific amendments to/refinements of the Call-Off Contract terms	N/A
Personal Data and Data Subjects	Annex 1 of Schedule 7 is being used.
Intellectual Property	N/A
Social Value	To support the delivery of Social Value through Governmental contracts, the Supplier has provided its FY23 Corporate Sustainability Report. The Supplier will help the Buyer to work towards net zero greenhouse gas emissions and to support environmental

	protection and improvement, in line with the Supplier's 2023 CSR commitment to be fully powered by renewable energy by 2026 and to have net zero emissions (CO2e) by 2030. The Supplier can measure and report on the carbon emissions from MongoDB usage and sharing these on the invoice statement.

1. Formation of contract

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

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

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

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

2. Background to the agreement

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

Signed	**Supplier**	**Buyer**
Name	Redacted: FOI SECTION 40 PERSONAL INFORMATION	Redacted: FOI SECTION 40 PERSONAL INFORMATION
Title	Redacted: FOI SECTION 40 PERSONAL INFORMATION	Redacted: FOI SECTION 40 PERSONAL INFORMATION
Signature	Redacted: FOI SECTION 40 PERSONAL INFORMATION	Redacted: FOI SECTION 40 PERSONAL INFORMATION

Date		

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

Customer Benefits

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

G-Cloud 13 Customer Benefit Record

Part B: Terms and conditions

1. Call-Off Contract Start date and length

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

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

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

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 24 months.

2. Incorporation of terms

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

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 10 (Force majeure)
- 5.3 (Continuing rights)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)

- 17 (Bribery and corruption)
- 18 (Freedom of Information Act)
- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)
- 24 (Conflicts of interest and ethical walls)
- 25 (Publicity and branding)
- 26 (Equality and diversity)
- 28 (Data protection)
- 31 (Severability)
- 32 and 33 (Managing disputes and Mediation)
- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

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

2.2.1 a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'

2.2.2 a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'

2.2.3 a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

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

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

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

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

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

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

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

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

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

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

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

5. Due diligence

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

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

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

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

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

6. Business continuity and disaster recovery

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

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

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

7. Payment, VAT and Call-Off Contract charges

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

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

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

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

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

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

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

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

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

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

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

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

9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.

9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.

9.8 The Supplier will be liable for the payment of any:

9.8.1 premiums, which it will pay promptly

9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

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

11. Intellectual Property Rights

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

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

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

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

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

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

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

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

(a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;

(b) alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;

(c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and

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

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

11.6.1 rights granted to the Buyer under this Call-Off Contract

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

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

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

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

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

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

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

11.8.2 other material provided by the Buyer necessary for the Services

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

12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

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

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

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

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

13. Buyer data

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

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

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

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

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

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

13.6.1 the principles in the Security Policy Framework:

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

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

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

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

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

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

13.6.6 Buyer requirements in respect of AI ethical standards.

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

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

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

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

14. Standards and quality

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

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

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

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

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN

Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

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

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

16. Security

16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the

Buyer's written approval of) a Security Management Plan and an Information Security

Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.

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

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

16.4 Responsibility for costs will be at the:

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

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

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

16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:

https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

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

17. Guarantee

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

17.1.1 an executed Guarantee in the form at Schedule 5

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

18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

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

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

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

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

18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)
- 24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability),

  24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

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

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

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

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

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

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

19.5.5 work with the Buyer on any ongoing work

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

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

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

20. Notices

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

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

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

21. Exit plan

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

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

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

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

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

21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own governance process. Where the Buyer is a

central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

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

21.6.2 there will be no adverse impact on service continuity

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

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

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

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

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

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

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

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

22. Handover to replacement supplier

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than 30 consecutive days, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

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

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

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

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

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

24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause 24.2 will not be taken into consideration.

25. Premises

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

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

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

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

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

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

25.5.2 comply with Buyer requirements for the conduct of personnel

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

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

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an

Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

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

29.2.1 the activities they perform

29.2.2 age

29.2.3 start date

29.2.4 place of work

29.2.5 notice period

29.2.6 redundancy payment entitlement

29.2.7 salary, benefits and pension entitlements

29.2.8 employment status

29.2.9 identity of employer

29.2.10 working arrangements

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.

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

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

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

29.5.1 its failure to comply with the provisions of this clause

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

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

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

30. Additional G-Cloud services

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

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

31. Collaboration

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

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

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

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

32. Variation process

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

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

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

33. Data Protection Legislation (GDPR)

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

Schedule 1: Services

The following Services are included under this Call Off Contract:

- MongoDB Atlas Enterprise Package

(the "**MongoDB Atlas Enterprise Package")**

- MongoDB: Consulting
- Training: Private Training Class per Day

(together, the "**Professional Services**")

,.

Professional Services: All work can only proceed following Buyer signature on an agreed Statement of Work. The utilisation of the Professional Services will be managed via a Professional Services log.

This Call Off Contract Order Form incorporates the Statement of Work # DEPAR-231128-A, - **See Annex 1 to Schedule 1.**

MongoDB Atlas Enterprise Package - See Annex 2 to Schedule 1.

Atlas is a database as a service from MongoDB, providing all of the features of the database, without the operational heavy lifting required for any new application. Atlas is available on-demand through a pay-as-you-go model and billed on an hourly basis, letting you focus on what you do best.

MongoDB: Consulting - See Annex 3 to Schedule 1.

We offer custom consulting projects to provide guidance outside the scope of our other consulting offerings. MongoDB consulting engineers can assist with all phases of implementations, such as installation, testing, deployment architecture, and best practices reviews. Consultants can work with your project team during critical phases of projects. For Further detail refer to Statement of Work # DEPAR-231128-A (at Annex 1 to Schedule 1).

Training: Private Training Class per Day - See Annex 4 to Schedule 1.

Build in-house MongoDB experts with structured classes taught live by MongoDB instructors and consultants. Private Training provides classrooms exclusive to your teams, with tailored agendas on your defined schedule. MongoDB Private Training day equals one day of private class for up to 12 participants. Training can be delivered on-site or virtually.

Reporting

As part of our ongoing Supplier Relationship Management cadence, both Parties will reasonably agree 4 Key Performance Indicators (one specific to Social Value) and appropriate metrics which we will monitor and report on a quarterly basis.

Annex 1 to Schedule 1:

Statement of Work # DEPAR-231128-A

Redacted: FOI SECTION 43 COMMERCIAL INFORMATION

Exhibit A
Contract Change Order

Customer Name	[customer name]	**Requested by**	[customer contact]
SOW Id	[SOW Id]	**CCO Id**	[SOW Id-CCO#]
Original Order Form	[Order Form]	**CCO Order Form**	[CCO Order Form]

Contract Change Order	
Date	
Requested by	
Impact on	n Scope n Budget n Timeline n Other:
Change description	[describe the reason for the change]
Consequences	[describe what's going to change (scope, budget and/or timeline, and in what manner)]
Investment	[describe required financial investment, if applicable]

Approval	
[Customer name]	MongoDB
Name:	Name:
Title:	Title:
Date:	Date:

Annex 2 to Schedule 1:

MongoDB Atlas Enterprise Package

MongoDB Atlas Enterprise

Industry leaders and startups alike rely on MongoDB Atlas, a fully managed database as a service platform for MongoDB, and round-the-clock support to run their deployments with the utmost conJdence.

MongoDB Atlas Enterprise includes access to our proactive support team for end to end MongoDB coverage; enterprise security features; a suite of advanced software that allows you to easily explore, manipulate, and perform analytics on your data; and access to on-demand training resources.

What's Inside?

- **Fully Managed Database as a Service.** Easily deploy, manage, and scale your MongoDB deployments using built in operational and security best practices that we — the company behind the database — have learned from optimizing thousands of deployments from small to massive across startups and the Fortune 100.
- **Deep Monitoring, Query Optimization, & Customizable Alerts.** MongoDB Atlas allows you to visualize and act on over 100 performance metrics, track database performance in real-time, and receive automated suggestions on how to improve slow-running queries. Atlas also allows you to set up custom alerts that trigger when metrics go out of range so you can uncover performance issues before they affect your users.
- **Proactive Support.** MongoDB Atlas Enterprise provides access to proactive, consultative support. The same team that builds the database helps you throughout your entire application lifecycle. Customers can ask MongoDB experts an unlimited number of questions, 24 x 365, globally. Our support team also acts as an extension of your team by diagnosing, detecting, and troubleshooting potential issues before they turn into problems for your deployment.
- **Enterprise-Grade Security.** Enterprise security features such as LDAP integration, encryption key management, and granular database auditing grant you more control over how you secure your database environment.
- **Fully Managed Backups.** Protect your business by protecting your data. An optional add-on service to MongoDB Atlas, our fully managed backup solution for MongoDB is the only solution that offers point-in-time recovery, the ability to query your backups, and synchronized snapshots of sharded clusters.
- **GUI for MongoDB.** MongoDB Compass enables you to visually explore your schema and data, build and run ad hoc queries in seconds, ensure data quality, and analyze and optimize performance. MongoDB Compass also features a powerful visual editor designed to streamline your interactions with your data.
- **Advanced Analytics.** The BI connector for Atlas is a turnkey service that lets you use your Atlas clusters as data sources for your SQL-based BI and analytics platforms. Seamlessly create the visualizations and dashboards that will help you extract the insights and hidden value in your multi-structured data.
- **On-Demand Training.** Get access to our online training, and at your pace. Developers and ops teams can improve their MongoDB skills on-demand from wherever they want, whenever it Jts their schedule.

MongoDB Atlas Enterprise Features

Fully Managed Database as a Service	✓
Seamless Upgrades & Auto-Healing	✓
Fully Elastic; Scale Up & Down with Ease & Zero Downtime	✓
Deep Monitoring & Customizable Alerts	✓
Highly Secure by Default	✓
Encryption Key Management	✓
Granular Database Auditing	✓
LDAP Integration	✓
Continuous Backups with Point-in-Time Recovery*	✓
Uptime SLA	✓
MongoDB Compass	✓
BI Connector for Atlas	✓
On-Demand Access to MongoDB University	✓
Support Response SLA	1 hour
Support Availability	24 x 365

*Customers have the option to pay for backup a la carte

What's Next?

For more information, please visit mongodb.com/atlas or contact us at sales@mongodb.com.

Case Studies (mongodb.com/customers)
Resource Center (mongodb.com/resource-center)
Free Online Training (university.mongodb.com)
Documentation (docs.mongodb.com)
MongoDB Stitch Serverless Platform(mongodb.com/stitch)
MongoDB Mobile (mongodb.com/products/mobile)
MongoDB Enterprise Download (mongodb.com/download)
MongoDB Atlas Database as a Service for MongoDB (mongodb.com/cloud)

mongoDB

US 866-237-8815 • INTL +1-650-440-4474 • info@mongodb.com

Annex 3 to Schedule 1:

MongoDB: Consulting

MongoDB: Consulting

We're your strategic partner to help you bring ideas to life, whether you just need a technical advice to push your project forward, or you need an entire development team to execute on your applications.

We offer custom consulting projects for those looking for guidance outside of the scope of our other consulting offerings. MongoDB consulting engineers can assist with all phases of implementations, such as installation, configuration, testing, performance tuning, deployment architecture, and best practices reviews. The consultants can work as a part of your project team during critical phases of projects on an ongoing or recurring basis.

GCloud RateCard

Role	Day Rate (GBP)
Principal Consulting Engineer	2700
Senior Consulting Engineer	2290
Senior Project Manager	2000

MongoDB

Annex 4 to Schedule 1:

Training: Private Training Class per Day

Training: Private Training Class per Day

Our Training addresses common barriers to MongoDB adoption and success

Build in-house MongoDB experts with structured classes taught live by MongoDB instructors and consultants. Private Training provides classrooms exclusive to your teams, with tailored agendas on your defined schedule. MongoDB Private Training day equals one day of private class for upto 12 participants. Training can be delivered on-site or virtually.

GCloud RateCard

Role	Day Rate (GBP)
Training: Private Training Class per Day	3900

MongoDB

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:

Service Description: MongoDB Atlas Enterprise Package

Service ID: 9591 1102 5794 492

Based on the Credit consumption forecast, it is anticipated that a total quantity of Redacted: FOI SECTION 43 COMMERCIAL INFORMATION MongoDB Atlas Enterprise Package credits is estimated to be consumed over the term of the contract.

Atlas credits will be purchased over the 36-months term.

MongoDB will invoice the Buyer monthly in arrears for the Buyer's use of the MongoDB Atlas subscription during the subscription period and will be charged at the unit price of GBP 0.80 per credit.

Estimated Usage

Subscription	Service ID	Term (months)	Dates	Forecast Qty (credits)	ACTUAL Unit Price (GBP)	Estimated Total (GBP)
MongoDB ATLAS Enterprise Package	95911102 5794492	36	Feb 1, 2024 - Jan 31, 2027	Redacted: FOI SECTION 43 COMMERCIAL INFORMATION	£0.80	Redacted: FOI SECTION 43 COMMERCIAL INFORMATION

The Buyer may commence use of the MongoDB Atlas service purchased in this Order Form from the beginning of the latest unbilled period or, if no prior usage, up to 30 days before the start of the subscription period.

Minimum monthly support payments apply to MongoDB Atlas Enterprise Package subscriptions. Monthly charges will be the greater of $1,500 or a usage-based fee in accordance with the following tiered pricing model:

Redacted: FOI SECTION 43 COMMERCIAL INFORMATION

Professional Services – (includes **-** MongoDB: Consulting & Training: Private Training Class per Day)

Upon execution of this Call Off Contract, the Supplier will invoice the Buyer Redacted: FOI SECTION

43 COMMERCIAL INFORMATION for the Professional Services purchased in this Call Off Contract. Professional Services expire at the end of the Call-Off Contract term, with no further obligation from the Supplier.

Subscription	Service ID	Term (months)	Dates	Total (GBP)
MongoDB: Consulting	5520 2729 2439 363	36	February 1, 2024 - January 31, 2027	Redacted: FOI SECTION 43 COMMERCIAL INFORMATION
Training: Private Training Class per Day	9444 1361 2840 759	36	February 1, 2024 - January 31, 2027	Redacted: FOI SECTION 43 COMMERCIAL INFORMATION

The Professional Services Cost is broken down in the table below:

Redacted: FOI SECTION 43 COMMERCIAL INFORMATION

Business Hours
Unless the Supplier agrees otherwise, the Supplier provide Consulting Services Monday through Friday during the business hours of 9am to 5pm in the time zone of your location,

excluding holidays observed by the Supplier. For work performed on weekends or holidays, the Buyer will pay overtime rate of two times of the consulting rate as agreed for the Consulting Services. One day of Consulting Services is eight hours.

Cancellation Policy
The Buyer may reschedule a services engagement more than 5 business days before the scheduled start date without penalty. If the Buyer reschedules a services engagement between 1 and 5 business days before the scheduled start date, The Buyer will forfeit 25% of the scheduled days and will be charged 100% of the Supplier's non-refundable travel expenses unless otherwise mutually agreed upon in writing. If the Buyer reschedules a services engagement less than 1 business day before the scheduled start, the Buyer will forfeit 50% of the scheduled days and will be charged 100% of the Supplier's non-refundable travel expenses unless otherwise mutually agreed upon in writing.

Travel & Expenses

The Services will be delivered by the Supplier to the Buyer remotely.

Any travel required throughout the duration of the Call-Off contract term, must be agreed upon in writing between the parties and included within the Call-Off Contract via a contract Variation, aligned to DWP Travel and Expenses Policy (a copy of which is included as Exhibit C to this Call Off Contract).

MongoDB: Consulting
Upon execution of this Call Off Contract, the Supplier will invoice the Buyer in full for the Consulting Services purchased in this Call Off Contract. Consulting Services expire at the end of the subscription period indicated on this Call Off Contract (the "Subscription Period") with no further obligation from the Supplier. The Consulting Services shall be fully delivered upon the earlier of (i) delivery of all days included in the subscription or (ii) expiration of the Subscription Period. New information or the Buyer's failure to fulfill its responsibilities described in the SOW associated with the Consulting Services purchased in this Call Off Contract may cause a change in scope or timeline that will require the Buyer to purchase additional Consulting Services. Consulting Services are accepted upon delivery. If any conflict exists between the acceptance terms in the Statement of Works and this Call Off Contract, this Call Off Contract controls.

Training: Private Training Class per Day
Each Training: Private Training Class per Day subscription includes one day of private training for up to 12 attendees. The Buyer may choose any of the private training courses described at https://www.mongodb.com/products/training/instructor-led. The Buyer will work with the Supplier to schedule the training at a mutually agreed upon date. The Buyer and the Supplier will agree in advance whether the training will be delivered remotely or on site. Attendees may not record, copy or distribute the training course or any accompanying course materials. Any days not used during the subscription period expire.

Additional Purchases
During the term of this Call Off Contract, the Buyer may purchase NTSE subscriptions (Platform Service ID Number - 5450 1327 4476 968 Named Technical Services Engineer (the "**NTSE Services**")), at the then current list price as per the G-Cloud Framework ("**Additional Purchases**"). Any subscription for NTSE Services as part of an Additional Purchase will be coterminous with the subscriptions set forth in this Call Off Contract

Schedule 3: Collaboration agreement

Not Used

Schedule 4: Alternative clauses

1. Introduction

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

2. Clauses selected

2.1 The Customer 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 Customer 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 his best endeavours to ensure that in his employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract he promotes equality of treatment and opportunity between:

a. persons of different religious beliefs or political opinions
b. men and women or married and unmarried persons
c. persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)
d. persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)
e. persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)
f. persons of different ages
g. 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 Customer 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:

a. the issue of written instructions to staff and other relevant persons
b. the appointment or designation of a senior manager with responsibility for equal opportunities
c. training of all staff and other relevant persons in equal opportunities and harassment matters
d. 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 Customer as soon as possible in the event of:

A. 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
B. 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 Period 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 Customer 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 Customer. 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 Customer 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 Customer 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 Customer in relation to same.

2.6 Health and safety

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

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

2.6.3 The Supplier will notify the Customer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Customer 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 Customer 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 Customer 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 Customer for any loss arising
directly from a breach of this obligation (including any diminution of monies received by the Customer under any insurance policy).

2.7.2 If during the Call-Off Contract Period 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
Customer 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 Customer's cost and the Supplier will (at no additional cost to the Customer) provide any help the Customer 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

[A Guarantee should only be requested if the Supplier's financial standing is not enough on its own to guarantee delivery of the Services. This is a draft form of guarantee which can be used to procure a Call Off Guarantee, and so it will need to be amended to reflect the Beneficiary's requirements]

This deed of guarantee is made on [**insert date, month, year]** between:

(1) [**Insert the name of the Guarantor]** a company incorporated in England and Wales with number [insert company number] whose registered office is at [i**nsert details of the guarantor's registered office**] [or a company incorporated under the Laws of
[**insert country**], registered in [**insert country**] with number [**insert number**] at [**insert place of registration**], whose principal office is at [**insert office details**]]('Guarantor'); in favour of
and

(2) The Buyer whose offices are [**insert Buyer's official address**] ('Beneficiary')

Whereas:

(A) The guarantor has agreed, in consideration of the Buyer entering into the Call-Off Contract with the Supplier, to guarantee all of the Supplier's obligations under the Call-Off Contract.

(B) It is the intention of the Parties that this document be executed and take effect as a deed.

[Where a deed of guarantee is required, include the wording below and populate the box below with the guarantor company's details. If a deed of guarantee isn't needed then the section below and other references to the guarantee should be deleted.

Suggested headings are as follows:

- Demands and notices
- Representations and Warranties
- Obligation to enter into a new Contract
- Assignment
- Third Party Rights
- Governing Law
- This Call-Off Contract is conditional upon the provision of a Guarantee to the Buyer from the guarantor in respect of the Supplier.]

Guarantor company	[**Enter Company name**] **'Guarantor'**
Guarantor company address	[**Enter Company address**]
Account manager	[**Enter Account Manager name]**
	Address: [**Enter Account Manager address]**
	Phone: [**Enter Account Manager phone number]**
	Email: [**Enter Account Manager email**]
	Fax: [**Enter Account Manager fax** if applicable]

In consideration of the Buyer entering into the Call-Off Contract, the Guarantor agrees with the Buyer as follows:

Definitions and interpretation

In this Deed of Guarantee, unless defined elsewhere in this Deed of Guarantee or the context requires otherwise, defined terms will have the same meaning as they have for the purposes of the Call-Off Contract.

Term	Meaning
Call-Off Contract	Means [the Guaranteed Agreement] made between the Buyer and the Supplier on [insert date].
Guaranteed Obligations	Means all obligations and liabilities of the Supplier to the Buyer under the Call-Off Contract together with all obligations owed by the Supplier to the Buyer that are supplemental to, incurred under, ancillary to or calculated by reference to the Call-Off Contract.
Guarantee	Means the deed of guarantee described in the Order Form (Parent Company Guarantee).

References to this Deed of Guarantee and any provisions of this Deed of Guarantee or to any other document or agreement (including to the Call-Off Contract) apply now, and as amended, varied, restated, supplemented, substituted or novated in the future.

Unless the context otherwise requires, words importing the singular are to include the plural and vice versa.

References to a person are to be construed to include that person's assignees or transferees or successors in title, whether direct or indirect.

The words 'other' and 'otherwise' are not to be construed as confining the meaning of any following words to the class of thing previously stated if a wider construction is possible.

Unless the context otherwise requires:

- reference to a gender includes the other gender and the neuter
- references to an Act of Parliament, statutory provision or statutory instrument also apply if amended, extended or re-enacted from time to time
- any phrase introduced by the words 'including', 'includes', 'in particular', 'for example' or similar, will be construed as illustrative and without limitation to the generality of the related general words

References to Clauses and Schedules are, unless otherwise provided, references to Clauses of and Schedules to this Deed of Guarantee.

References to liability are to include any liability whether actual, contingent, present or future.

Guarantee and indemnity

The Guarantor irrevocably and unconditionally guarantees that the Supplier duly performs all of the guaranteed obligations due by the Supplier to the Buyer.

If at any time the Supplier will fail to perform any of the guaranteed obligations, the Guarantor irrevocably and unconditionally undertakes to the Buyer it will, at the cost of the Guarantor:

- fully perform or buy performance of the guaranteed obligations to the Buyer
- as a separate and independent obligation and liability, compensate and keep the Buyer compensated against all losses and expenses which may result from a failure by the Supplier to perform the guaranteed obligations under the Call-Off Contract

As a separate and independent obligation and liability, the Guarantor irrevocably and unconditionally undertakes to compensate and keep the Buyer compensated on demand against all losses and expenses of whatever nature, whether arising under statute, contract or at common Law, if any obligation guaranteed by the guarantor is or becomes unenforceable, invalid or illegal as if the obligation guaranteed had not become unenforceable, invalid or illegal provided that the guarantor's liability will be no greater than the Supplier's liability would have been if the obligation guaranteed had not become unenforceable, invalid or illegal.

Obligation to enter into a new contract

If the Call-Off Contract is terminated or if it is disclaimed by a liquidator of the Supplier or the obligations of the Supplier are declared to be void or voidable, the Guarantor will, at the request of the Buyer, enter into a Contract with the Buyer in the same terms as the Call-Off Contract and the obligations of the Guarantor under such substitute agreement will be the same as if the Guarantor had been original obligor under the Call-Off Contract or under an agreement entered into on the same terms and at the same time as the Call-Off Contract with the Buyer.

Demands and notices

Any demand or notice served by the Buyer on the Guarantor under this Deed of Guarantee will be in writing, addressed to:

[**Enter Address of the Guarantor in England and Wales**]

[**Enter Email address of the Guarantor**

representative] For the Attention of [**insert details**]

or such other address in England and Wales as the Guarantor has notified the Buyer in writing as being an address for the receipt of such demands or notices.

Any notice or demand served on the Guarantor or the Buyer under this Deed of Guarantee will be deemed to have been served if:

- delivered by hand, at the time of delivery
- posted, at 10am on the second Working Day after it was put into the post

- sent by email, at the time of despatch, if despatched before 5pm on any Working Day, and in any other case at 10am on the next Working Day

In proving Service of a notice or demand on the Guarantor or the Buyer, it will be sufficient to prove that delivery was made, or that the envelope containing the notice or demand was properly addressed and posted as a prepaid first class recorded delivery letter, or that the fax message was properly addressed and despatched.

Any notice purported to be served on the Buyer under this Deed of Guarantee will only be valid when received in writing by the Buyer.

Beneficiary's protections

The Guarantor will not be discharged or released from this Deed of Guarantee by:

- any arrangement made between the Supplier and the Buyer (whether or not such arrangement is made with the assent of the Guarantor)
- any amendment to or termination of the Call-Off Contract
- any forbearance or indulgence as to payment, time, performance or otherwise granted by the Buyer (whether or not such amendment, termination, forbearance or indulgence is made with the assent of the Guarantor)
- the Buyer doing (or omitting to do) anything which, but for this provision, might exonerate the Guarantor

This Deed of Guarantee will be a continuing security for the Guaranteed Obligations and accordingly:

- it will not be discharged, reduced or otherwise affected by any partial performance (except to the extent of such partial performance) by the Supplier of the Guaranteed Obligations or by any omission or delay on the part of the Buyer in exercising its rights under this Deed of Guarantee
- it will not be affected by any dissolution, amalgamation, reconstruction, reorganisation, change in status, function, control or ownership, insolvency, liquidation, administration, appointment of a receiver, voluntary arrangement, any legal limitation or other incapacity, of the Supplier, the Buyer, the Guarantor or any other person
- if, for any reason, any of the Guaranteed Obligations is void or unenforceable against the Supplier, the Guarantor will be liable for that purported obligation or liability as if the same
  were fully valid and enforceable and the Guarantor were principal debtor

- the rights of the Buyer against the Guarantor under this Deed of Guarantee are in addition to, will not be affected by and will not prejudice, any other security, guarantee, indemnity or other rights or remedies available to the Buyer

The Buyer will be entitled to exercise its rights and to make demands on the Guarantor under this Deed of Guarantee as often as it wishes. The making of a demand (whether effective, partial or defective) relating to the breach or non-performance by the Supplier of any Guaranteed Obligation will not preclude the Buyer from making a further demand relating to the same or some other Default regarding the same Guaranteed Obligation.

The Buyer will not be obliged before taking steps to enforce this Deed of Guarantee against the Guarantor to:

- obtain judgment against the Supplier or the Guarantor or any third party in any court
- make or file any claim in a bankruptcy or liquidation of the Supplier or any third party
- take any action against the Supplier or the Guarantor or any third party
- resort to any other security or guarantee or other means of payment

No action (or inaction) by the Buyer relating to any such security, guarantee or other means of payment will prejudice or affect the liability of the Guarantor.

The Buyer's rights under this Deed of Guarantee are cumulative and not exclusive of any rights provided by Law. The Buyer's rights may be exercised as often as the Buyer deems expedient. Any waiver by the Buyer of any terms of this Deed of Guarantee, or of any Guaranteed Obligations, will only be effective if given in writing and then only for the purpose and upon the terms and conditions on which it is given.

Any release, discharge or settlement between the Guarantor and the Buyer will be conditional upon no security, disposition or payment to the Buyer by the Guarantor or any other person being void, set aside or ordered to be refunded following any enactment or Law relating to liquidation, administration or insolvency or for any other reason. If such condition will not be fulfilled, the Buyer will be entitled to enforce this Deed of Guarantee subsequently as if such release, discharge or settlement had not occurred and any such payment had not been made. The Buyer will be entitled to retain this security before and after the payment, discharge or satisfaction of all monies, obligations and liabilities that are or may become due owing or incurred to the Buyer from the Guarantor for such period as the Buyer may determine.

Representations and warranties

The Guarantor hereby represents and warrants to the Buyer that:

- the Guarantor is duly incorporated and is a validly existing company under the Laws of its place of incorporation
- has the capacity to sue or be sued in its own name
- the Guarantor has power to carry on its business as now being conducted and to own its Property and other assets

- the Guarantor has full power and authority to execute, deliver and perform its obligations under this Deed of Guarantee and no limitation on the powers of the Guarantor will be exceeded as a result of the Guarantor entering into this Deed of Guarantee
- the execution and delivery by the Guarantor of this Deed of Guarantee and the performance by the Guarantor of its obligations under this Deed of Guarantee including entry into and performance of a Call-Off Contract following Clause 3) have been duly authorised by all necessary corporate action and do not contravene or conflict with:
    - the Guarantor's memorandum and articles of association or other equivalent constitutional documents, any existing Law, statute, rule or Regulation or any judgment, decree or permit to which the Guarantor is subject
    - the terms of any agreement or other document to which the Guarantor is a party or which is binding upon it or any of its assets
    - all governmental and other authorisations, approvals, licences and consents, required or desirable

This Deed of Guarantee is the legal valid and binding obligation of the Guarantor and is enforceable against the Guarantor in accordance with its terms.

Payments and set-off

All sums payable by the Guarantor under this Deed of Guarantee will be paid without any set-off, lien or counterclaim, deduction or withholding, except for those required by Law. If any deduction or withholding must be made by Law, the Guarantor will pay that additional amount to ensure that the Buyer receives a net amount equal to the full amount which it would have received if the payment had been made without the deduction or withholding.

The Guarantor will pay interest on any amount due under this Deed of Guarantee at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgment.

The Guarantor will reimburse the Buyer for all legal and other costs (including VAT) incurred by the Buyer in connection with the enforcement of this Deed of Guarantee.

Guarantor’s acknowledgement

The Guarantor warrants, acknowledges and confirms to the Buyer that it has not entered into this
Deed of Guarantee in reliance upon the Buyer nor been induced to enter into this Deed of Guarantee by any representation, warranty or undertaking made by, or on behalf of the Buyer, (whether express or implied and whether following statute or otherwise) which is not in this Deed of Guarantee.

Assignment

The Buyer will be entitled to assign or transfer the benefit of this Deed of Guarantee at any time to any person without the consent of the Guarantor being required and any such assignment or transfer will not release the Guarantor from its liability under this Guarantee.

The Guarantor may not assign or transfer any of its rights or obligations under this Deed of Guarantee.

Severance

If any provision of this Deed of Guarantee is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision will be severed and the remainder of the provisions will continue in full force and effect as if this Deed of Guarantee had been executed with the invalid, illegal or unenforceable provision eliminated.

Third-party rights

A person who is not a Party to this Deed of Guarantee will have no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Deed of Guarantee. This Clause does not affect any right or remedy of any person which exists or is available otherwise than following that Act.

Governing law

This Deed of Guarantee, and any non-Contractual obligations arising out of or in connection with it, will be governed by and construed in accordance with English Law.

The Guarantor irrevocably agrees for the benefit of the Buyer that the courts of England will have jurisdiction to hear and determine any suit, action or proceedings and to settle any dispute which may arise out of or in connection with this Deed of Guarantee and for such purposes hereby irrevocably submits to the jurisdiction of such courts.

Nothing contained in this Clause will limit the rights of the Buyer to take proceedings against the Guarantor in any other court of competent jurisdiction, nor will the taking of any such proceedings in one or more jurisdictions preclude the taking of proceedings in any other jurisdiction, whether concurrently or not (unless precluded by applicable Law).

The Guarantor irrevocably waives any objection which it may have now or in the future to the courts of England being nominated for this Clause on the ground of venue or otherwise and agrees not to claim that any such court is not a convenient or appropriate forum.

[The Guarantor hereby irrevocably designates, appoints and empowers [**enter the Supplier name**] [or a suitable alternative to be agreed if the Supplier's registered office is not in England or Wales] either at its registered office or on fax number [**insert fax number**] from time to time to act as its authorised agent to receive notices, demands, Service of process and any other legal summons in England and Wales for the purposes of any legal action or

proceeding brought or to be brought by the Buyer in respect of this Deed of Guarantee. The Guarantor hereby irrevocably consents to the Service of notices and demands, Service of process or any other legal summons served in such way.]

IN WITNESS whereof the Guarantor has caused this instrument to be executed and delivered as a Deed the day and year first before written.

EXECUTED as a DEED by

[**Insert name of the Guarantor**] acting by [**Insert names**]

Director

Director/Secretary

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform).
Audit	An audit carried out under the incorporated Framework Agreement clauses.

Background IPRs	For each Party, IPRs: • owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes • created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.

Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.

Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.

Confidential Information	Data, Personal Data and any information, which may include (but isn't limited to) any: ● information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above ● other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the UK GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.

Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
Data Subject	Takes the meaning given in the UK GDPR
Default	Default is any: • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .

End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.

ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-todate version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-fortax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.

Force Majeure	A force Majeure event means anything affecting either Party's performance of their obligations arising from any: ● acts, events or omissions beyond the reasonable control of the affected Party ● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare ● acts of government, local government or Regulatory Bodies ● fire, flood or disaster and any failure or shortage of power or fuel ● industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: ● any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain ● any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure ● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into ● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.13 together with the Framework Schedules.

Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or
	defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.

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

Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.

Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.

Insolvency event	Can be: ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium ● a Dun & Bradstreet rating of 10 or less
Intellectual Property Rights or IPR	Intellectual Property Rights are: ● copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information ● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the supplier's own limited company ● a service or a personal service company ● a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).

IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or Buyer's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.

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

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

Personal Data	Takes the meaning given in the UK GDPR.
Personal Data Breach	Takes the meaning given in the UK GDPR.
Platform	The government marketplace where Services are available for Buyers to buy.
Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK GDPR.

Prohibited act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.

Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.

Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call- Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.

Services	The services ordered by the Buyer as set out in the Order Form.
Service data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.

Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controlsche ck-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.

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

Supplier staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7: UK GDPR Information

This schedule reproduces the annexes to the UK GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract and clause and schedule

references are to those in the Framework Agreement but references to CCS have been amended.

Annex 1: Processing Personal Data

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

The contact details of the Buyer's Data Protection Officer are: Redacted: FOI SECTION 40 PERSONAL INFORMATION

The contact details of the Supplier's Data Protection Officer are: Redacted: FOI SECTION 40 PERSONAL INFORMATION

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

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

Description	**Details**
Identity of Controller for each Category of Personal Data	The Buyer is Controller and the Supplier is Processor The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, Buyer is the Controller and the Supplier is the Processor of the Personal Data recorded below: • Any Personal Data that Buyer uploads into the Cloud Services that is processed by Supplier

Duration of the Processing	Until the expiration or termination of the Call Off Contract in accordance with its terms.
Nature and purposes of the Processing	The provision of the Cloud Services to the Buyer in accordance with the Call Off Contract.
Type of Personal Data	Any Buyer Personal Data uploaded to the Cloud Services by Buyer.

Categories of Data Subject	Staff and members of the public.

Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	Buyer may retrieve or delete all Buyer Personal Data upon expiration or termination of the Call Off Contract. Upon termination of the Call Off Contract or upon your request, Supplier will delete any Buyer Personal Data not deleted by Buyer, unless Supplier is legally required to store the Buyer Personal Data.

Annex 2: Joint Controller Agreement

1. 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 all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

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

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

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

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

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

2. Undertakings of both Parties

2.1 The Supplier and the Buyer each undertake that they shall:

(a) report to the other Party every [**insert number**] months on:

(i) the volume of Data Subject Request (or purported Data Subject 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 Contract 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 Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. 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) take all reasonable steps 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 ’s 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;

(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 Data Loss Event having taken account of the:

(i) nature of the data to be protected;
(ii) harm that might result from a Data Loss Event;
(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

(i) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

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

3. Data Protection Breach

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

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

(b) all reasonable assistance, including:

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

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

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

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

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

hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

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

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

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

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

4. Audit

4.1 The Supplier shall permit:

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

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

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

5. Impact Assessments

5.1 The Parties shall:

(a) provide all reasonable assistance to the each other to prepare any data protection impact assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

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

6. ICO Guidance

6.1 The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

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]

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

(a) if in the view of the Information Commissioner, the Buyer is responsible for the

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

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

cooperation and access to conduct a thorough audit of such Personal Data Breach; or

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

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

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

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

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

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

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

8. Termination

8.1 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 Contract by issuing a Termination Notice to the Supplier in accordance with Clause 5.1.

9. Sub-Processing

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

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, 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

10.1 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 Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy

EXHIBIT A TO THE CALL OFF CONTRACT

MongoDB Service Level Agreement

MongoDB Atlas Service Level Agreement

Last updated: June 23, 2021. To see what has changed, click here.

MongoDB will use commercially reasonable efforts to maximize the availability of MongoDB Atlas, and provides performance standards as detailed below. This Service Level Agreement ("SLA") applies only to MongoDB Atlas deployments at level M10 or above that have been up for a minimum of 24 hours, and does not apply to any other product offered by MongoDB. We will provide at least 90 days' advance notice for adverse changes to this SLA.

If we do not achieve and maintain the Monthly Uptime Percentages set forth in the table below, then you may be eligible for a Service Credit.

Monthly Uptime Percentage	Service Credit
< 99.995% but equal to or greater than 99.0%	10%
< 99.0%	25%
< 95.0%	100%

Definitions

As used herein, "month" refers to a calendar month.

"Applicable Monthly Service Fees" means the total fees paid by you for a given MongoDB Atlas cluster during the month in which Downtime occurred.

"Downtime" is calculated per MongoDB Atlas cluster on a monthly basis and is the total number of minutes during the month that the entire MongoDB Atlas cluster was unavailable. A minute is considered unavailable if all of your continuous attempts to establish a connection to the MongoDB Atlas cluster within the minute fail. Downtime does not include partial minutes of unavailability or scheduled downtime for maintenance and upgrades.

"Monthly Uptime Percentage" is calculated per MongoDB Atlas cluster on a monthly basis and is calculated as:

$$\frac{(\textit{total minutes in month} - \textit{Downtime})}{\textit{total minutes in month}} \times 100$$

Any MongoDB Atlas cluster deployed for only part of the month is assumed to be 100% available for the portion of the month that it is not deployed.

"Service Credit" is the percentage of the Applicable Monthly Service Fees to be credited to you if MongoDB approves your claim, as set forth in the table above.

Customer Obligations

To be eligible for a Service Credit:

1. You must log a support ticket with MongoDB within 24 hours of first becoming aware of an event that impacts service availability.
2. You must submit your claim and all required information by the end of the month immediately following the month in which the Downtime occurred.
3. You must include all information necessary for MongoDB to validate your claim, including: (i) a detailed description of the events resulting in Downtime, including your request logs that document the errors and corroborate your claimed outage (with any confidential or sensitive information in the logs removed or replaced with asterisks); (ii) information regarding the time and duration of the Downtime; (iii) the number and location(s) of affected users (if applicable); and (iv) descriptions of your attempts to resolve the Downtime at the time of occurrence.
4. You must reasonably assist MongoDB in investigating the cause of the Downtime and processing your claim.
5. You must comply with your applicable MongoDB Atlas service agreement, applicable MongoDB Atlas documentation and any advice from our support team.

Service Credits

We will process claims within 45 days of receipt. If we determine that you have satisfied the customer obligations above and that none of the below limitations apply to your claim, we will grant you a Service Credit.

We will apply any Service Credit to a future invoice or payment for the MongoDB Atlas cluster that experienced the Downtime. Service Credits will not be applied to fees for any other MongoDB Atlas cluster.

Service Credits are your sole and exclusive remedy under this SLA.

Limitations

Downtime does not include, and you will not be eligible for a Service Credit for, any performance or availability issue that results from:

1. Factors outside of our reasonable control, such as natural disaster, war, acts of terrorism, riots, government action, or a network or device failure at your site or between your site and MongoDB Atlas;
2. Services, hardware, or software provided by a third party, such as cloud platform services on which MongoDB Atlas runs;
3. Use of your password or equipment to access our network
4. Your or any third party's (a) improper use, scaling or configuration of MongoDB Atlas, or (b) failure to follow appropriate security practices; or
5. MongoDB's Beta Offerings.

EXHIBIT B TO THE CALL OFF CONTRACT

MongoDB Technical Standards

Technical and Organizational Security Measures

Register Now

Please register to be notified of any changes to this page. If a change occurs, you will receive an email to the address that you provide.

Last updated: August 31, 2022. To see what has changed, click here.

These Technical and Organizational Security Measures ("Security Measures") are incorporated into and form part of your applicable agreement with MongoDB with respect to your use of MongoDB Atlas (the "Agreement"). These Security Measures also apply to MongoDB Atlas for Government, as modified by the MongoDB Atlas for Government Addendum to the Agreement.

The Security Measures set out the security features, processes, and controls applicable to MongoDB Atlas, including configurable options available to Customer, which employ industry standard information security best practices.

1. Definitions

The following terms have the following meanings when used in the Security Measures. Any capitalized terms that are not defined in the Security Measures have the meaning provided in your Agreement.

1.1. "Cloud Provider" means Amazon Web Services (AWS), Microsoft Azure (Azure), or Google Cloud Platform (GCP), as selected by Customer.

1.2. "Customer Data" means any data you or your end users upload into MongoDB Atlas.

1.3. "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.

1.4. "Information Security Program" means MongoDB's written security program, policies, and procedures that set forth the administrative, technical, and physical safeguards designed to protect Customer Data.

1.5. "MongoDB Atlas Cluster" means each replica set or sharded cluster of data-bearing nodes running the MongoDB database software that is managed by MongoDB Atlas, subject to your selected configurations.

1.6. "MongoDB Atlas Project" means one or more associated MongoDB Atlas Clusters with a shared set of authorization and network configurations.

1.7. "MongoDB Systems" means MongoDB's internal infrastructure, including development, testing, and production environments, for MongoDB Atlas.

1.8. "Privileged User" means a select MongoDB employee or third-party contractor who has been granted unique authority to access Customer Data or MongoDB Systems as required to perform their job function.

1.9. "Security Incident Response Plan" means MongoDB's documented protocols for evaluating suspected security threats and responding to confirmed Data Breaches and other security incidents.

2. Information Security Program Overview.

2.1. General. MongoDB maintains a comprehensive written Information Security Program to establish effective administrative, technical, and physical safeguards for Customer Data, and to identify, detect, protect against, respond to, and recover from security incidents. MongoDB's Information Security Program complies with applicable Data Protection Law and is aligned with the NIST Cyber Security Framework (NIST). Additionally, MongoDB Atlas is certified against ISO 27001:2013, ISO 27017:2015, ISO 27018:2019, SOC 2 Type II, Payment Card Industry Data Security

Standard v.3.2.1, and Cloud Security Alliance (CSA) Security, Trust, Assurance, and Risk (STAR) Level 2. MongoDB Atlas has also undergone a HIPAA examination validated by a qualified third-party assessor and can be configured to build HIPAA compliant applications.

2.2. Maintenance and Compliance. MongoDB's Information Security Program is maintained by a dedicated security team, led by our Chief Information Security Oficer. MongoDB monitors compliance with its Information Security Program, and conducts ongoing education and training of personnel to ensure compliance. The Information Security Program is reviewed and updated at least annually to reflect changes to our organization, business practices, technology, services, and applicable laws and regulations. We will not alter or modify the Information Security Program in a way that materially weakens or compromises the effectiveness of its security controls.

2.3. MongoDB Personnel Controls.

2.3.1. Background Checks. MongoDB performs industry standard background checks on all MongoDB employees as well as any third-party contractor with access to Customer Data or MongoDB Systems.

2.3.2. Personnel Obligations. Any Privileged User authorized to access Customer Data is required to commit in writing to information security and confidentiality obligations that survive termination and change of employment. MongoDB maintains a formal disciplinary procedure for violations by MongoDB personnel of its security policies and procedures.

2.3.3. Training. Upon hire and subsequently at least once per year, Privileged Users authorized to access Customer Data undergo required training on specific security topics, including phishing, secure coding, insider threats, and the secure handling of Customer Data and personally identifiable information. Further, MongoDB implements mandatory, role-specific training for Privileged Users who are authorized to access Customer Data. MongoDB maintains records of training occurrence and content. In addition to these mandatory trainings, MongoDB offers employees additional training

resources, such as internal security awareness and education groups and hackathons.

2.4. Third Parties. MongoDB maintains and adheres to a documented process for the evaluation and approval of third-party service providers prior to onboarding, which includes appropriate due diligence regarding each third party's security processes and controls. We require third parties to contractually commit to confidentiality, security responsibilities, security controls, and data reporting obligations, and we perform ongoing targeted due diligence on a quarterly basis.

2.5. Security Contact. If you have security concerns or questions, you may contact us via your normal Support channels, via support.mongodb.com, or by emailing security@mongodb.com.

3. MongoDB Atlas Security Controls.

3.1. Data Centers and Physical Storage. MongoDB Atlas runs on AWS, Azure, and GCP, and you control which Cloud Provider to use for deploying your MongoDB Atlas Clusters. Each Cloud Provider is responsible for the security of its data centers, which are compliant with a number of physical security and information security standards detailed at the Cloud Provider's respective websites:

- https://aws.amazon.com/security/
- https://www.microsoft.com/en-us/trustcenter/security/azure-security
- https://cloud.google.com/security/

At least twice per year, each of our Cloud Providers is subject to due diligence performed by MongoDB or third-party auditors, which includes obtaining and reviewing security compliance certifications.

In addition to selecting which Cloud Provider to use, you also control the region where your MongoDB Atlas Clusters are deployed. This gives you the flexibility to decide where your Customer Data is physically stored, and you may choose to deploy your Customer Data in a specific geographic region (for example, only within the European Union or only within the United States).

3.2. Encryption.

3.2.1. Encryption in Transit. All MongoDB Atlas network trafic is protected by Transport Layer Security (TLS), which is enabled by default and cannot be disabled. Customer Data that you transmit to MongoDB Atlas, as well as Customer Data transmitted between nodes of your MongoDB Atlas Cluster, is encrypted in transit using TLS. You can select which TLS version to use for your MongoDB Atlas Clusters, with TLS 1.2 being the recommended default and a minimum key length of 128 bits.

3.2.1.1. Key Management Procedures for Encryption in Transit. All encryption in transit is supported by the use of OpenSSL FIPS Object Module. We maintain documented cryptography and key management guidelines for the secure transmission of Customer Data, and we configure our TLS encryption key protocols and parameters accordingly. MongoDB's key management procedures include: (i) generation of keys with approved key length; (ii) secure distribution, activation and storage, recovery and replacement, and update of keys; (iii) recovery of keys that are lost, corrupted, or expired; (iv) backup/archive of keys; (v) maintenance of key history; (vi) allocation of defined key activation and deactivation dates; (vii) restriction of key access to authorized individuals; and (viii) compliance with legal and regulatory requirements. When a key is compromised, it is revoked, retired, and replaced to prevent further use (except for limited use of that compromised key to remove or verify protections). Keys are protected in storage by encryption and are stored separately from encrypted data. TLS certificates are obtained from a major, widely trusted third-party public certificate authority. In the course of standard TLS key negotiation for active sessions, ephemeral session keys are generated which are never persisted to disk, as per the design of the TLS protocol.

3.2.2. Encryption at Rest. Upon creation of a MongoDB Atlas Cluster, by default, Customer Data is encrypted at rest using AES-256 to secure all volume (disk) data. That process is automated by the transparent disk encryption of your selected Cloud Provider, and the Cloud Provider fully manages the encryption keys. You may also choose to enable database-level encryption via the WiredTiger Encrypted Storage Engine (using AES-256), as well as to bring your own encryption key with AWS

Key Management Service (KMS), GCP KMS, or Azure Key Vault (KV).

3.2.3. Encryption in Use. MongoDB Atlas also supports automatic encryption of individual data fields of Customer Data before they are sent to MongoDB Atlas. If you enable this client-side field level encryption feature for a selected data field, an application-side component built into the MongoDB drivers encrypts that field of Customer Data before leaving the driver to be sent to MongoDB Atlas, and only decrypts it upon return to the application once inside the driver. With respect to the Customer Data for which you enable client-side field level encryption, MongoDB Atlas never sees your unencrypted Customer Data and you control the encryption keys, which you can secure using any KMIP-compliant key management service.

3.3. Network Connectivity Options.

3.3.1. Network Isolation. You may choose to deploy your MongoDB Atlas Clusters in a dedicated virtual environment or a shared multi-tenant system. Dedicated MongoDB Atlas Clusters are deployed in a VPC (for AWS and GCP) or VNet (for Azure) that fully isolates your Customer Data and is configured to prevent inbound network access from the internet. Each such MongoDB Atlas VPC or VNet utilizes security groups that act as a virtual firewall for your dedicated MongoDB Atlas Clusters.

3.3.2. Atlas IP Access List. In order to allow inbound network access to your MongoDB Atlas VPC or VNet, you must configure an Atlas IP Access List to enable specific networks to connect to the MongoDB Atlas Clusters within your MongoDB Atlas Project. Unless the Atlas IP Access List for a MongoDB Atlas Project includes a specific network's IP addresses, network trafic is prevented from accessing your MongoDB Atlas Clusters in that MongoDB Atlas Project.

3.3.3. Virtual Private Cloud Peering. You may enable peering between your MongoDB Atlas VPC or VNet to your own dedicated application tier virtual private network with the Cloud Provider of your choice (VPC or VNet). Peering permits you to route encrypted trafic between your MongoDB Atlas VPC or VNet and your own application tier VPC or VNet privately, rather than traversing the public internet. Subject to

the capabilities of your selected Cloud Provider, you may also choose to peer your MongoDB Atlas VPC or VNet to your application tier VPC or VNet across regions.

3.3.4. Private Endpoints. MongoDB Atlas also supports private endpoints on AWS using the AWS PrivateLink feature and on Azure using the Azure Private Link feature. If you enable this feature for any MongoDB Atlas Cluster, that MongoDB Atlas Cluster will only allow a one-way connection from your AWS VPC or Azure VNet to the MongoDB Atlas Cluster and that MongoDB Atlas Cluster cannot initiate connections back to your AWS VPC or Azure VNet. Private endpoints also enable you to reach your MongoDB Atlas Cluster transitively over the network from other application tier AWS VPCs and Azure VNets that you have peered with the private endpoint, or through your own self-managed virtual private network including via AWS DirectConnect and Azure ExpressRoute.

3.4. Configuration Management. The MongoDB Atlas environment, including our production environment and your MongoDB Atlas Clusters, leverages configuration management systems to fully automate configuration based on one-time decisions that are securely applied to new and existing environments to ensure consistency every time. Our production environment and your MongoDB Atlas Clusters use in-house built machine images with secure configuration management applied via industry standard automation software, which includes hardening steps.

4. Access Controls.

4.1. Customer Access. MongoDB Atlas supports multiple authentication and authorization options and methods to give you the flexibility to meet your individualized requirements and needs. You are responsible for understanding the security configuration options available to you and the impact of your selected configurations on your MongoDB Atlas environment, which consists of a web application administrative interface ("MongoDB Atlas UI") and any MongoDB Atlas Cluster you deploy. MongoDB Atlas provides you with configurable authentication and authorization options for both the MongoDB Atlas UI and your MongoDB Atlas Clusters.

4.1.1. MongoDB Atlas UI Authentication and Authorization. User credentials for the MongoDB Atlas UI are stored using industry standard and audited one-way hashes. The MongoDB Atlas UI supports multi-factor authentication (MFA), including a security key/biometrics option that enables you to use hardware security keys or built-in authenticators. The MongoDB Atlas UI also supports federated authentication functionality for Single Sign-On (SSO) utilizing Security Assertion Markup Language (SAML).

4.1.2. MongoDB Atlas Cluster Authentication and Authorization. Authentication control for a MongoDB Atlas Cluster is enabled by default with the Salted Challenge Response Authentication Mechanism (SCRAM). You may choose to manage user authentication with self-managed X.509 certificates or through AWS IAM Users or Roles. MongoDB Atlas allows you to define permissions for individual users or applications in order to restrict the Customer Data that is accessible in a query. Further, you may choose to assign each user a MongoDB Atlas Project-specific role, which authorizes that user to perform specific actions on the MongoDB Atlas Clusters within that MongoDB Atlas Project. The MongoDB Atlas UI allows you to tailor your access controls by combining multiple roles and privileges for particular users. You can review, limit, and revoke user access to your MongoDB Atlas Clusters at any time. MongoDB Atlas also provides you with the ability to manage user authentication and authorization using your own Lightweight Directory Access Protocol (LDAP) server over TLS. A single LDAP over TLS (LDAPS) configuration applies to all MongoDB Atlas Clusters in a MongoDB Atlas Project.

4.1.3. Credential Requirements. As part of the configuration options, you may establish minimum password requirements (e.g., length, complexity) through your identity provider after federating authentication to the MongoDB Atlas UI via SAML and to the MongoDB Atlas Clusters via LDAPS.

4.1.4. Customer Database Auditing. MongoDB Atlas offers granular auditing that monitors actions in your MongoDB Atlas environment and is designed to prevent and detect any unauthorized access to Customer Data, including create, read, update, and delete (CRUD) operations, encryption key management, and role-based access controls. You are

responsible for enabling database auditing and selecting the users, roles, groups, and event actions that you want to audit.

4.2. MongoDB Personnel Access to MongoDB Atlas Clusters.

4.2.1. Privileged User Access. As a general matter, MongoDB personnel do not have authorization to access your MongoDB Atlas Clusters. Only a small group of Privileged Users are authorized to access your MongoDB Atlas Clusters in rare cases where required to investigate and restore critical services. MongoDB adheres to the principle of "least privilege" with respect to those Privileged Users, and any access is limited to the minimum time and extent necessary to repair the critical issue. Privileged Users may only access your MongoDB Atlas Clusters via a gated process that uses a bastion host, requires MFA both to log in to our MongoDB Systems and to establish a Secure Shell connection (SSH) via the bastion host, and requires approval by MongoDB senior management.

4.2.2. Restricting MongoDB Personnel Access. MongoDB Atlas provides you with the option to entirely restrict access by all MongoDB personnel, including Privileged Users, to your MongoDB Atlas Clusters. If you choose to restrict such access and MongoDB determines that access is necessary to resolve a particular support issue, MongoDB must first request your permission and you may then decide whether to temporarily restore Privileged User access for up to 24 hours. You can revoke the temporary 24-hour access grant at any time. Enabling this restriction may result in increased time for the response and resolution of support issues and, as a result, may negatively impact the availability of your MongoDB Atlas Clusters. If you enable client-side field level encryption, even Privileged Users will be unable to access Customer Data within your MongoDB Atlas Clusters in the clear unless you provide MongoDB with the encryption keys.

4.2.3. Credential Requirements. Privileged User accounts may only be used for privileged activities, and Privileged Users must use a separate account to perform non-privileged activities. Privileged User accounts may not use shared credentials. The password requirements described in Section 4.3.3 also apply to Privileged User accounts.

4.2.4. Access Review and Auditing. MongoDB reviews Privileged User access authorization on a quarterly basis. Additionally, we revoke a Privileged User's access when it is no longer needed, including within 24 hours of that Privileged User changing roles or leaving the company. We also log any access by MongoDB personnel to your MongoDB Atlas Clusters. Audit logs are retained for at least six years, and include a timestamp, actor, action, and output. MongoDB utilizes a combination of automated and human review to scan those audit logs.

4.3. MongoDB Personnel Access to MongoDB Systems.

4.3.1. General. MongoDB's policies and procedures regarding access to MongoDB Systems adhere to the principles of role-based access control (RBAC), least privilege, and separation of duties. In accordance with these principles, with respect to MongoDB Atlas, MongoDB developers are only granted access to our development environments, and access to our production environment is limited to Privileged Users with appropriate authorizations. We review access authorizations to MongoDB Systems on a quarterly basis and we review any changes to authorizations for Privileged Users immediately. As part of the employee off-boarding process, access to MongoDB Systems is revoked within 24 hours of an employee's departure.

4.3.2. Access to MongoDB Atlas Production Environment. Our backend production environment that runs MongoDB Atlas is only accessible by a dedicated group of Privileged Users whose privileges must be approved by senior management. Privileged Users may only access our backend production environment via a bastion host and doing so requires MFA both to log in and to establish a SSH via the bastion host.

4.3.3. Credential Requirements. All MongoDB personnel passwords must conform to industry-standard complexity rules. Additionally, MFA is mandatory for all MongoDB personnel and cannot be disabled.

4.4. Physical Controls at MongoDB Ofices. As noted in Section 3.1, Customer Data is deployed at the data centers of your selected Cloud Provider, and not at facilities owned or operated by MongoDB. At MongoDB ofices, we follow industry best practices to employ physical security controls that are appropriate to the level

of risk posed by the information stored and the nature of operations at our ofices. In our ofices, we: (i) issue access cards for all personnel through formal provisioning and approval processes; (ii) limit access to restricted areas to personnel with a need to access those areas to carry out their job functions; (iii) require visitors to sign in, execute a non-disclosure agreement, and be escorted in all non-public spaces; (iv) employ surveillance systems to monitor activity at points of entry from public spaces; and (v) revoke personnel access within 12 hours of termination.

4.5. Secure Deletion of Customer Data. If you terminate a MongoDB Atlas Cluster, it will become unavailable to you immediately and any Cloud Backup associated with that MongoDB Atlas Cluster will be terminated. MongoDB may retain a copy of the Customer Data stored in the terminated MongoDB Atlas Cluster for up to 5 days. If you terminate Cloud Backups, all snapshots will become unavailable to you immediately and it may take up to 24 hours for the Customer Data contained in the snapshots to become unrecoverable. When you terminate a MongoDB Atlas Project, the master key used to encrypt Customer Data is securely wiped, rendering all Customer Data effectively unrecoverable. If you choose to use MongoDB Atlas Online Archive, you can delete the entire archive, or pre-defne automatic deletion dates for different data sections within MongoDB Atlas Online Archive to help automate any applicable retention restrictions or policies.

5. MongoDB Systems Security.

5.1. Separation of Production and Non-Production Environments. MongoDB Atlas has strict separation between production and non-production environments. Our MongoDB Atlas production environment, your MongoDB Atlas Clusters, and your Customer Data are never utilized for non-production purposes. Our non-production environments are utilized for development, testing, and staging. MongoDB also maintains frewalls to achieve strict separation of our MongoDB Atlas production environment and MongoDB's internal network.

5.2. Sotware Development Lifecycle. MongoDB has a dedicated security team, reporting to the Chief Information Security Oficer, that leads security initiatives in the sotware development lifecycle (SDLC). We develop new products and features in a multistage process using industry standard methodologies that include defned

security acceptance criteria and align with NIST and OWASP guidance. The SDLC includes regular code reviews, documented policies and procedures for tracking and managing all changes to our code, continuous integration of source code commits, code versioning, static and dynamic code analysis, vulnerability management, threat modeling, and bug hunts, as well as automated and manual source code analysis.

5.3. Monitoring and Alerting. MongoDB monitors the health and performance of MongoDB Atlas without needing to access your MongoDB Atlas Clusters. MongoDB maintains a centralized log management system for the collection, storage, and analysis of log data for our MongoDB Atlas production environment and your MongoDB Atlas Clusters. We use this information for health monitoring, troubleshooting, and security purposes, including intrusion detection. We maintain our log data for at least six years, and we utilize a combination of automated scanning, automated alerting, and human review to monitor the data.

5.4. Vulnerability Management.

5.4.1. MongoDB Atlas Vulnerability Scanning. MongoDB maintains a documented vulnerability enumeration and management program that identifies internet-accessible company assets, scans for known vulnerabilities, evaluates risk, and tracks issue remediation. We conduct quarterly scans of both the underlying systems upon which MongoDB Atlas is deployed, as well as all third-party code integrated into our products. MongoDB's vulnerability management policy requires individual engineering teams to identify known vulnerabilities in system components, and develop remediation timeframes commensurate to the severity of an identified issue. We also utilize automated tooling in conjunction with monitoring security bulletins for relevant software and libraries, and implement patches if security issues are discovered.

5.4.2. Vulnerability Remediation. MongoDB uses a central company-wide ticketing system to track all security issues until remediation. We implement patches to our operating system and applications on a need-to-update basis, as determined in accordance with the Common Vulnerability Scoring System (CVSS). We are also a Mitre CVE Numbering Authority (CNA). Development tasks for all patches, bug fixes, and new features

are defined as issues for specific target releases and are deployed to production only after completing requisite checkpoints, including quality assurance testing, staged deployment, and management review.

5.5. Penetration Testing and Internal Risk Assessments. MongoDB Atlas undergoes regular reviews from both internal and external security teams.

5.5.1. External Testing. Our MongoDB Atlas production environment is subject to an external penetration test by a nationally recognized security firm at least once per calendar year. Upon request, we will provide you with a summary letter of engagement that includes the number of high, medium, and low issues identified, but due to the sensitivity of the information gathered during these tests, we cannot allow customers to perform testing of our production platform. Application-level security testing uses a standard application assessment methodology (e.g., OWASP). Additionally, external engagements with security consultants may include social engineering and phishing testing.

5.5.2. Internal Testing. Internally, MongoDB Atlas undergoes periodic risk assessments, including technical vulnerability discovery and analysis of business risks and concerns. The MongoDB security team is also routinely involved in source code review, architecture review, code commit peer review, and threat modeling.

6. Contingency Planning.

6.1. High Availability and Failover. Every MongoDB Atlas Cluster is deployed as a self-healing replica set that provides automatic failover in the event of a failure. Replica set members are automatically provisioned by MongoDB Atlas across multiple availability zones within a region, providing resilience to localized site failures. All replica set members are full data-bearing nodes, ensuring majority writes in the event of single node failure and higher resilience during recovery. Concurrent writes across replica sets occur in real time. MongoDB Atlas also offers multi-region and multi-cloud deployment options.

6.2. Backups. MongoDB Atlas offers Cloud Backups, which use the native snapshot functionality of your selected Cloud Provider to locally back up your Customer Data. You may enable Cloud Backups when you create or modify a MongoDB Atlas Cluster, and you have control over how oten a Cloud Backup is captured and the length of time for which Cloud Backups are retained. Cloud Backup snapshots are stored with your selected Cloud Provider in the primary region of your MongoDB Atlas Cluster. All Cloud Backups are encrypted at rest and you may choose to use self-managed keys with the WiredTiger Encrypted Storage Engine. You may also optionally enable Continuous Cloud Backups with point-in-time recovery stored on our encrypted S3 buckets.

6.3. Business Continuity and Disaster Recovery. MongoDB maintains a documented business continuity and disaster recovery ("BCDR") plan that aligns with ISO/IEC 22301:2019. Our BCDR plan includes: (i) clearly defined roles and responsibilities; (ii) availability requirements for customer services, including recovery point objectives (RPOs) and recovery time objectives (RTOs); and (iii) backup and restoration procedures. We review, update, and test our BCDR plan at least annually. In the event of an incident that triggers the BCDR plan, the RPO will depend on your impacted MongoDB Atlas Cluster and backup configurations. You can test how your application handles a replica set failover at any time using the MongoDB Atlas UI or API.

7. Incident Response and Communications.

7.1. Security Incident Response Plan. As part of the Information Security Program, MongoDB maintains an established Security Incident Response Plan that aligns with NIST and ISO/IEC 27001:2013. In the event that MongoDB becomes aware of a Data Breach or other security incident, MongoDB will follow the Security Incident Response Plan, which includes: (i) clearly defined roles and responsibilities, including designation of a security incident task force; (ii) reporting mechanisms; (iii) procedures for assessing, classifying, containing, eradicating, and recovering from security incidents; (iv) procedures and timeframes for required notifications to relevant authorities and customers; (v) procedures for forensic investigation and preservation of event and system log data; and (vi) a process for post-incident and resolution analysis designed to prevent future similar incidents. The Security Incident Response Plan

is reviewed, updated, and tested annually, including a security tabletop exercise at least once per year.

7.2. Security Incident Tracking. MongoDB maintains a comprehensive security incident tracking system that aligns with ISO/IEC 27001:2013 and documents: (i) incident type and suspected cause; (ii) whether there has been unauthorized or unlawful access, disclosure, loss, alteration, or destruction of data; (iii) if so, the categories of data affected by the incident, including categories of personal information; (iv) the time when the incident occurred or is suspected to have occurred; and (v) the remediation actions taken.

7.3. Customer Communications. MongoDB will notify you without undue delay if we become aware of any Data Breach. Taking into account the information available to us, such notice will include a description of the nature and cause of the Data Breach and the expected resolution time. To the extent possible, we will subsequently update you with information regarding evaluation of the root cause, potential impact, remediation actions taken, and actions planned to prevent a future similar event.

8. Audit Reporting.

8.1. Third-Party Certifications and Audit Reports. Upon request, and subject to the confidentiality obligations set forth in the Agreement, we will make available to you (or your independent, third-party auditor) information regarding MongoDB's compliance with the security obligations set forth in these Security Measures in the form of third-party certifications and audit reports.

8.2. Security Questionnaires. No more than once per year, we will complete a written security questionnaire provided by you regarding the controls outlined in these Security Measures.

EXHIBIT C TO THE CALL OFF CONTRACT

DWP Travel & Expense Policy

DWP Travel & Expenses Policy (Jan 23 policy)

1. The following principles and guidance are extracted from the Buyers expenses policy and are only intended to be a summary of the key areas and further guidance can be provided by the Buyer upon request from the Supplier, as the policy may change from time to time.

2. When making a claim for any payment the Supplier shall provide the Buyer with reasonably requested documentary evidence of actual expenditure to support the claim.

3. Supplier resources / Contractors can claim expenses for business travel and accommodation where they have to make a journey to another DWP office or to an official meeting not on DWP premises. Claims for meals/ subsistence cannot be made as Supplier resources / contractor day rates are deemed sufficient to cover such costs. Contractors cannot make claims for any meals.

HOTEL ACCOMODATION
Eligibility

1. You can stay overnight in hotel accommodation for a maximum of 30 nights.

2. Hotel accommodation should only be booked for the actual nights you stay in the accommodation and will not be payable during any absence from work or time away from the accommodation unless you are off sick and:

- are certified medically unfit to travel; or
- you have a short period of illness of 3 days or less and no appreciable savings would be made if you returned home during your illness.

3. Hotel accommodation can only be used for the night of your last day of duty if you were unable to return to your home by 20:00 hours and subsequently stayed a further night.

HOTEL ROOM EXPENDITURE LIMITS
The following regional maximum expenditure limits are in place:

- Overnight stay - London £150
- Rest of the country (except London) - £100

RAIL TRAVEL
1. First Class rail travel is not permitted. Economy class only.

2. Restricted/Advance Purchase tickets must be booked for your journey. As well as being the cheapest option this will also ensure that you have a definite train booked and a seat for your journey(s). ‘Anytime’ tickets should only be purchased where they are the cheapest available ticket.

TAXIS
1. Staff must always consider whether travelling by taxi is a necessity, having considered alternative travel methods, business needs, sustainability issues and increased public scrutiny of expenses and cost.

When Can I use a Taxi?

2. Taxis can only be used where one of the following applies:

- Heavy luggage has to be handled
- A taxi can be shared with colleagues and there is a saving over public transport costs
- There is no suitable method of public transport
- It is necessary due to a long term health problem
- There is a risk to personal safety
- Exceptionally, the saving of official time is important

3. You can only use a taxi where the fare will be under £50 per person per journey. There are no exceptions to this limit and the limit overrides the authorised use reasons above. You cannot claim reimbursement for any tips or gratuities.

AIR TRAVEL (including International Air Travel)
Key Policy Points

1. Business journeys must only be booked when meeting in person is essential.

2. Air travel can be authorised where, taking into account the full cost and duration of the journey including travel to/from the airport, and potential overnight stays saved, it offers better value for money than alternative methods.

3. The cheapest ticket which meets the travel requirements must be purchased. In most circumstances this will be an Advance or Fixed ticket.

4. Flights within the UK must be Economy class. When you are flying overseas and flight is less than 2.5 hours you must travel in economy class

5. When you are flying overseas and the flight is over 2.5 hours you should agree the most appropriate class of travel taking into account the requirement to spend responsibly and protect the reputation of the department.

6. Business Class tickets and any tickets costing more than £1,000 should not be booked without prior approval from the Permanent Secretary. You must not book 1st class tickets in any circumstances

7. You must not request lounge access unless this is specifically approved as a necessity, after giving consideration to the extra cost and the actual amount of working time intending to spend in the lounge