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	548472460453157
Call-Off Contract reference	W84458
Call-Off Contract title	CrowdStrike
Call-Off Contract description	The NHSBSA requires an incident response service to help in responding to a suspected computer security incident.
Start date	30/06/2023
Expiry date	28/07/2023
Call-Off Contract value	£38,366.30
Charging method	To be invoiced at the end of each calendar month
Purchase order number	TBA

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	NHS Business Services Authority Stella House Goldcrest Way Newcastle upon Tyne Tyne and Wear NE15 8NY

To the Supplier	SOFTCAT PLC Solar House Fieldhouse Lane Marlow Buckinghamshire United Kingdom SL7 1LW Company No. 02174990
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: Commercial Officer

Name: [redacted]

Email: [redacted]

For the Supplier:

Title: Account Manager

Name: [redacted]

Email: [redacted]

Phone: [redacted]

Title: Account Manager (CrowdStrike)

Name: [redacted]

Email: [redacted]

Call-Off Contract term

Start date	This Call-Off Contract Starts on **30/06/2023** and is valid until 28/07/2023
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).
Extension period	Not Applicable

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 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: ● Professional services related to cyber security, such as incident response investigation, forensic services, tabletop exercises, and next generation penetration tests. ● Further detail is outlined in Annex 3 – SOW 1.
Additional Services	**Post-Engagement Data Retention Fees** Physical Evidence (e.g., removable media, hard drives) – to be provided 90 days from the completion of the engagement and priced at [redacted] per physical evidence device, if required. Virtual Evidence (e.g., system images, memory capture) and Falcon Forensics Collector data to be provided 90 days from the completion of the engagement and priced at [redacted] per GB (or any portion thereof), if required.
Location	The Services will be delivered remotely.

Quality and Technical Standards:	The quality and technical standards required for this Call-Off Contract are as defined in the Supplier's G-Cloud 13 Service Definition on the Digital Marketplace.
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are as defined in the Supplier's G-Cloud 13 Service Definition on the Digital Marketplace.
Onboarding	The onboarding plan for this Call-Off Contract is as defined in the Supplier's G-Cloud 13 Service Definition on the Digital Marketplace

Offboarding	The offboarding plan for this Call-Off Contract is as defined in the Supplier's G-Cloud 13 Service Definition on the Digital Marketplace
Collaboration agreement	Not Applicable

Limit on Parties' liability	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 125% of the charges payable per year. The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation, or damage to any Buyer Data will not exceed 125**%** of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). The annual total liability of the Supplier for all other Defaults will not exceed the greater of 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).

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)] ● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Buyer's responsibilities	The Buyer's obligations are outlined within Section 7 of Exhibit A of the CrowdStrike Terms & Conditions (Annex 4 – CrowdStrike terms and conditions).
Buyer's equipment	Not applicable.

Supplier's information

Subcontractors or partners	The following is a list of the Supplier's Subcontractors or Partners: • CrowdStrike Inc.

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 **via BACS.**
Payment profile	The payment profile for this Call-Off Contract is invoice at the end of each calendar month.
Invoice details	The Supplier will issue electronic invoices **monthly** in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.
Who and where to send invoices to	Invoices will be sent: Via email (preferred) to: [redacted] Or by post to: Stella House, Goldcrest Way, Newburn Riverside Park, Newcastle-Upon-Tyne, Tyne & Wear, NE15 8NY
Invoice information required	All invoices must include the Purchase Order Reference, as provided by the Buyer in the initial order.

Invoice frequency	Invoice will be sent to the Buyer monthly.
Call-Off Contract value	The total value of this Call-Off Contract is £38,366.30.
Call-Off Contract charges	The breakdown of the Charges is detailed in Schedule 2 – Call-Off Contract Charges.

Additional Buyer terms

Performance of the Service	● Covered under Annex 3 – SOW 1

Guarantee	Not used.
Warranties, representations	Not used.
Supplemental requirements in addition to the Call-Off terms	Not applicable.
Alternative clauses	These Alternative Clauses, which have been selected from Schedule 4, will apply: Not applicable.

Buyer specific amendments to/refinements of the Call-Off Contract terms	Not applicable.
Personal Data and Data Subjects	Confirm whether Annex 1 (and Annex 2, if applicable) of Schedule 7 is being used: Annex 1
Intellectual Property	Not applicable.
Social Value	As per the G-Cloud 13 supplier offering.

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	On and behalf of the NHSBSA	On and behalf of SOFTCAT PLC
	Signed via DocuSign on 12/07/2023	Signed via DocuSign on 13/07/2023

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.

2.6 The defined term 'Confidential Information' (as defined in Schedule 3 of the Framework Agreement) is deleted and replaced in its entirety by the following:

"means all confidential information (however recorded or preserved) disclosed by a Party to the other Party in connection with the Call-Off Contract, in all cases whether or not it is designated or marked as confidential, including but not limited to:

(a) the existence and terms of the Call-Off Contract and any other information concerning the Buyer's use of the Framework Agreement for the subject matter of this Call-Off Contract;

(b) any information that would be regarded as confidential by a reasonable business person relating to:

i. the business, assets, affairs, customers, clients, suppliers, or plans, intentions, or market opportunities of the disclosing Party; and

ii. the operations, processes, product information, know-how, designs, trade secrets, intellectual property rights or software of the disclosing Party;

(c) any information shared or developed by the Parties in the course of carrying out this Call-Off Contract including relating to or arising from any investigations carried out pursuant to the Call-Off Contract; and

(d) data including Personal Data which is shared under the Framework Agreement or this Call-Off Contract,

but shall not mean any Confidential Information that was, is or becomes available to the receiving Party on a non-confidential basis from a person who, to the receiving Party's knowledge, is not bound by a confidentiality agreement with the disclosing Party or otherwise prohibited from disclosing the information to the receiving Party.

2.7 The following new provisions will be deemed to be incorporated into clause 34 (Confidentiality):

34.10 Each Party reserves all rights in its Confidential Information. No rights or obligations in respect of a Party's Confidential Information other than those expressly stated in this Call-Off Contract are granted to the other Party, or to be implied from this Call-Off Contract.

34.11 On termination or expiry of this Call-Off Contract, each Party shall

(a) destroy or return to the other Party all documents and materials (and any copies) containing, reflecting, incorporating or based on the other Party's Confidential Information;

(b) erase all the other Party's Confidential Information from computer and communications systems and devices used by it, including such systems and data storage services provided by third parties (to the extent technically and legally practicable); and

(c) certify in writing to the other Party that it has complied with the requirements of this clause, provided that a recipient Party may retain documents and materials containing, reflecting, incorporating or based on the other Party's Confidential Information to the extent required by law or any applicable governmental or regulatory authority.

34.12 The provisions of this clause 34 shall survive for a period of five years from termination or expiry of 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-securityclassifications

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

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

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

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

13.6.6 Buyer requirements in respect of AI ethical standards.

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

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

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

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

14. Standards and quality

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

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

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

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

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

15. Open source

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

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

16. Security

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

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

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

16.4 Responsibility for costs will be at the:

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

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

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

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

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

17. Guarantee

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

17.1.1 an executed Guarantee in the form at Schedule 5

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

18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

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

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

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

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

18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)

- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)
- 24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability), 24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

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

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

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

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

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

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

19.5.5 work with the Buyer on any ongoing work

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

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

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

20. Notices

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

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

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

21. Exit plan

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

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

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

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

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

21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from 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 services shall meet the following requirements:

Requirement Type	Description
Incident Response Services	CrowdStrike will assist Customer with responding to a suspected computer security incident. CrowdStrike will help Customer perform the following phases of work.
Incident Response Triage	CrowdStrike shall, as needed: ○ Analyse data, including but not limited to: • Forensic images of disk and/or memory from systems of interest; • Data collected by CrowdStrike Tools; • Live response data from suspected systems of interest; • Logs from computer systems, including network traffic, firewalls, DNS and DHCP servers, authentication servers, VPN or remote access servers, and system logs; • Documentation of system and network architecture, tools and capabilities; • How the incident was detected and business concerns related to the incident; • Malware, attack tools, malicious software or documents, adversary tactics or other Threat Actor Data; ○ Provide, assist with the deployment of, and use CrowdStrike Tools (defined in section entitled CrowdStrike Tools) as well as use existing Customer tools to gather data for analysis; ○ Discuss the incident with Customer staff in remote or in-person meetings; ○ Perform this analysis on or off Customer's site; ○ Provide a summary of incident triage, with recommended next steps and effort estimates.

Investigation and Containment	CrowdStrike shall, as needed: ○ Determine compromised or accessed systems, develop a timeline of attacker activity, investigate the likely attack vector, and what data and user accounts may have been compromised or accessed; ○ Provide recommendations for containment actions and as directed, use CrowdStrike Tools to perform tactical containment actions, including but not limited to advanced information gathering (e.g., suspicious or unknown file collection) and actions such as removing malware, terminating processes, and removing or modifying a malicious Windows registry key or value; ○ Provide network analysis services; • Provide to Customer for use during the engagement Falcon Network (defined below in the section entitled CrowdStrike Tools) that monitor network traffic near Internet egress designated by Customer; • Help Customer's staff position and connect Falcon Network hardware (if any) to Customer's network; • Collect and analyze network traffic; ○ Provide containment and recovery recommendations to reduce Customer's attack surface, including, but not limited to: • Identifying unnecessary privileges; • Configuring logging, monitoring, and alerting; • Hardening configuration templates; • Implementing network segmentation; • Plan a remediation event to deny the attacker further access to Customer's environment;
Strategic Recommendations	○ CrowdStrike may produce recommendations for long-term continuous security posture improvement.
Status Reporting	During all phases, CrowdStrike will: ○ As requested, provide daily status updates verbally or by email, including information about activities performed, findings and their criticality, and plans for upcoming work; ¡ As requested, provide written weekly summary updates, reviewing tasks, issues and progress, and advising of the status of work and the budget;
Engagement Artifacts	CrowdStrike may, as requested, construct and present draft and final reports containing findings and observations. A report is initially delivered in a draft format and then discussed with Customer. The draft report is then revised and delivered as a final report if Customer has not requested revisions or provided questions regarding the report in 10 business days. CrowdStrike will conduct discussion and status meetings as defined above. The written engagement artifacts (report) may contain information summarizing the Services for an executive reader, as well as detailed technical information for a technical reader.

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:

Quantity	Description	Unit Price	Total Price
100	Crowdstrike Incident Response Services 12 months	[redacted]	[redacted]
1	Tools Fee for CrowdStrike Cloud Collector 12 months	[redacted]	[redacted]
		Subtotal (GBP)	**£38,366.30**
		Delivery	£0.00
		Total (GBP)	**£38,366.30**

Schedule 3: Collaboration agreement

Not used.

Schedule 4: Alternative clauses

Not used.

Schedule 5: Guarantee

Not used.

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

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

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

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

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

Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
Data Subject	Takes the meaning given in the UK GDPR
Default	Default is any: • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
DPA 2018	Data Protection Act 2018.

Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.

ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.

Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-todate version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-fortax
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: o under the Bribery Act 2010 o under legislation creating offences concerning Fraud o at common Law concerning Fraud o 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.

1.1 The contact details of the Buyer's Data Protection Officer are: [redacted] ([redacted])

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

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

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

Description	Details
Identity of Controller 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: • Prescription Data
Duration of the Processing	Approximately 4 weeks
Nature and purposes of the Processing	Supplier is reviewing the storage accounts containing the personal data so will have access to the data but not beneficial to their investigation to do so. They will not be transferring any data. Supplier will be taking snapshots/copies of the infrastructure, rather than the data itself.
Type of Personal Data	Prescription data

Categories of Data Subject	Customers, members of the general public, patients.
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	No data will be retained or captured.

Annex 2: Joint Controller Agreement

Not used.

Annex 3: Statement of Work

Statement of Work

FOR

Incident Response Services

Contains confidential information subject to non-disclosure requirements.

PREPARED FOR

NHS Business Services Authority

Stella House, Newcastle-Upon-Tyne,

NE158NY United Kingdom

PREPARED ON	SOW #
June 29, 2023	**1**

CROWDSTRIKE

Primary Contacts

Customer Contacts

Technical Contact

PARTY
NHS Business Services Authority

NAME
[redacted]

TITLE

PHONE

EMAIL
[redacted]

Billing Information

PARTY
Softcat plc Accounts Payable ("Reseller")

ADDRESS
Fieldhouse Lane, Marlow
Buckinghamshire, SL7 1LW
United Kingdom

PHONE
[redacted]

EMAIL
[redacted]

CrowdStrike Contacts

Services Sales Contact

[redacted]

Phone
[redacted]

Email Address
[redacted]

**If you are unsure if your email infrastructure may be compromised, consider sending us an email from a 3rd party email address (e.g., Gmail)*

EMAIL
[redacted]

PHONE
Regional Incident Response Hotlines:

North America:	1-855-276-9347
UK/ Ireland:	+44 800 0487187
Australia:	+61 (1800) 290-853
Japan:	000 800 170-5401
India:	+91 (1800) 040-3447
France:	+33 801840 073
Germany:	+49 (0800) 3252669

Statement of Work

This Statement of Work 1 ("SOW") is entered into by CrowdStrike, Inc., and any Affiliates performing hereunder, (collectively "CrowdStrike") and NHS Business Services Authority ("Customer") as of the last signature date below (the "SOW Effective Date") and forms a part of and is subject to the CrowdStrike Terms and Conditions located here[1] (the "Agreement"). Capitalized terms used in this SOW but not defined herein shall have the meaning set forth in the Agreement. Nothing in this SOW shall be construed as an amendment of the Agreement but is merely a supplement thereto. In the event of any inconsistency between this SOW and the Agreement, the latter shall prevail.

Scope of Work

Definition of Services

CrowdStrike will provide the following professional services (the "Services") to Customer.

Scope of Services

Incident Response Services

CrowdStrike will assist Customer with responding to a suspected computer security incident. CrowdStrike will help Customer perform the following phases of work.

Incident Response Triage

CrowdStrike shall, as needed:

- Analyze data, including but not limited to:
  - Forensic images of disk and/or memory from systems of interest;
  - Data collected by CrowdStrike Tools;
  - Live response data from suspected systems of interest;
  - Logs from computer systems, including network traffic, firewalls, DNS and DHCP servers, authentication servers, VPN or remote access servers, and system logs;
  - Documentation of system and network architecture, tools and capabilities;

[1] http://www.crowdstrike.com/terms

- How the incident was detected and business concerns related to the incident;
- Malware, attack tools, malicious software or documents, adversary tactics or other Threat Actor Data;

- Provide, assist with the deployment of, and use CrowdStrike Tools (defined in section entitled *CrowdStrike Tools*) as well as use existing Customer tools to gather data for analysis;
- Discuss the incident with Customer staff in remote or in-person meetings;
- Perform this analysis on or off Customer's site;
- Provide a summary of incident triage, with recommended next steps and effort estimates.

Investigation and Containment

CrowdStrike shall, as needed:

- Determine compromised or accessed systems, develop a timeline of attacker activity, investigate the likely attack vector, and what data and user accounts may have been compromised or accessed;
- Provide recommendations for containment actions and as directed, use CrowdStrike Tools to perform tactical containment actions, including but not limited to advanced information gathering (e.g., suspicious or unknown file collection) and actions such as removing malware, terminating processes, and removing or modifying a malicious Windows registry key or value;
- Provide network analysis services;
  - Provide to Customer for use during the engagement Falcon Network (defined below in the section entitled *CrowdStrike Tools*) that monitor network traffic near Internet egress designated by Customer;
  - Help Customer's staff position and connect Falcon Network hardware (if any) to Customer's network;
  - Collect and analyze network traffic;
- Provide containment and recovery recommendations to reduce Customer's attack surface, including, but not limited to:
  - Identifying unnecessary privileges;
  - Configuring logging, monitoring, and alerting;
  - Hardening configuration templates;
  - Implementing network segmentation;
  - Plan a remediation event to deny the attacker further access to Customer's environment;

Strategic Recommendations

CrowdStrike may produce recommendations for long-term continuous security posture improvement.

Status Reporting

During all phases, CrowdStrike will:

- As requested, provide daily status updates verbally or by email, including information about activities performed, findings and their criticality, and plans for upcoming work;
- As requested, provide written weekly summary updates, reviewing tasks, issues and progress, and advising of the status of work and the budget;

Engagement Artifacts

CrowdStrike may, as requested, construct and present draft and final reports containing findings and observations. A report is initially delivered in a draft format and then discussed with Customer. The draft report is then revised and delivered as a final report if Customer has not requested revisions or provided questions regarding the report in 10 business days. CrowdStrike will conduct discussion and status meetings as defined above. The written engagement artifacts (report) may contain information summarizing the Services for an executive reader, as well as detailed technical information for a technical reader.

Schedule and Change Management

Delivery Schedule

Work will begin on a mutually agreed upon date.

Change Management

CrowdStrike will notify Customer via email if any of the hourly estimates listed below will be exceeded. Customer is responsible for paying the Reseller fees for hours in excess of the estimate without the need for approvals beyond this signed SOW so long as all hours billed are within the scope of work described in this SOW. Any change to the scope of Services will be agreed upon in writing by CrowdStrike and Customer and Customer shall issue a corresponding order covering such fees with the Reseller in advance of the change and any additional fees associated therewith.

Time & Materials Minimum

CrowdStrike will charge Reseller, and Customer shall pay Reseller no fewer than 40 hours of professional services.

SOW Expiration

Customer has one year from SOW Effective Date to initiate the Services defined herein, otherwise this SOW is invalid and new terms must be established if services are requested.

Pricing

Fees

Customer is responsible for paying Reseller at the rate mutually agreed upon by Customer and Reseller for: (i) the number of hours worked by CrowdStrike, (ii) the CrowdStrike Tools and Post-Engagement Data Retention fees (if any), and (iii) expenses and travel time as described below. CrowdStrike will charge Reseller at the rate mutually agreed upon between CrowdStrike and Reseller for all of the above pursuant to quote number **Q-735851** dated June 29, 2023, provided to Reseller. Customer or CrowdStrike may provide a copy of this SOW to the Reseller.

Service	Estimated LOE[1]	Structure
Incident Response[2] **Estimate for initial Incident Triage**	[redacted]	[redacted]
Tools Fee for CrowdStrike Cloud Collectors[3] - Additional **fee** per platform	[redacted]	[redacted]
Expenses:		**Billed at actuals**

[1]The Level of Effort ("LOE") estimates provided for Professional Services performed on a Time and Material basis are estimates only and not a guaranteed time of completion.

[2] Actual Level of Effort ("LOE") will be updated based on Incident Response Triage. The LOE hours listed above will be leveraged for Services indicated herein, however, CrowdStrike's ability to perform all of these activities under the initial number of hours estimated is dependent on the level of complexity and scope of the breach.

[3] CrowdStrike Tools fee(s) shall be incurred on a per month basis beginning on the SOW Effective Date If Falcon Network Sensors (Corelight) are used, a refund will not be provided for partial use.

Travel & Expenses

CrowdStrike will charge actual expense amounts as incurred and will provide access to copies of receipts for those amounts upon request. CrowdStrike will not travel unless coordinated with the Customer. Travel expenses shall be reimbursed as follows: coach class airfare for flight times of 4 hours or less, economy plus for flight times between 4 and 8 hours, and business class airfare for flight times of more than 8 hours or for urgent international travel in support of incident response investigations; moderate class lodging; full size rental car; ground transportation including taxi or similar transportation services, parking, and/or mileage at the local government approved rate (e.g. IRS rates for U.S.); visa, work permit or similar fees; meal allowance of [redacted] Time spent traveling will be charged at [redacted] Travel time estimates are not included in Services time estimates.

Legal Request Fees

In the event CrowdStrike is legally required to respond to a request for information, and/or provide documents or testimony in connection with the Services as part of: (a) a legal proceeding to which the Customer is a party and CrowdStrike is not; or (b) a government or regulatory investigation of the Customer, the Customer shall: (i) pay all of CrowdStrike's reasonable and actual out of pocket legal fees and expenses (as evidenced by reasonably detailed invoices) in connection therewith, and (ii) pay the hourly rate set forth in this SOW (if no hourly rate is stated, then CrowdStrike's then-current hourly rate) for CrowdStrike's consultants' actual hours worked in responding to such requirement, including, time spent preparing for, and participating in, depositions and other testimony.

Taxes

Customer or Reseller is, to the extent mutually agreed between Customer and Reseller, responsible for the collection, remittance and reporting of all Value Added Taxes or similar taxes related to this SOW if work is performed outside the United States. Neither Customer nor Reseller is responsible for any income tax liability incurred by CrowdStrike.

If you are claiming a governmental exemption from sales tax, you must provide an official purchase order, or other documentation demonstrating direct payment from your agency, and we will confirm whether or not such an exemption is applicable in your particular jurisdiction. Purchases by individuals and reimbursed to them by a federal, state, or local government do not qualify for a sales tax exemption.

Invoicing and Payment

CrowdStrike will invoice Reseller at the end of each calendar month for: (i) the number of hours of Services, (ii) CrowdStrike Tools fees and/or Post-Engagement Data Retention fees, if any, (iii) travel time, if any, and (iv) actual expense amounts, all incurred in arrears. At the end of the engagement, remaining hours (if any) will be invoiced to the Reseller in order to meet the minimum set forth in the *Time and Materials Minimum* section.

Insurance

Incident Response Services sold through a Reseller are not eligible for rates specified under insurance panels.

Post-Engagement Data Retention Fees

If Customer directs CrowdStrike in writing to retain evidence/data beyond standard retention periods, Customer shall incur, and Reseller shall pay the Post-Engagement Data Retention fees set forth in the table below.

Post-Engagement Data Retention Fee(s) Table

Evidence/Data	If retention period is longer than…	Fees per month (or any portion thereof)
Physical Evidence **(e.g., removable media, hard drives)**	90 days from the completion of the engagement*	[redacted]
Virtual Evidence (e.g., system images, memory capture) and Falcon Forensics Collector data	90 days from the completion of the engagement*	[redacted]

***The "completion of the engagement" date will be specified in an email from CrowdStrike at the conclusion of the Services.**

CrowdStrike Tools

Definition

CrowdStrike may use one or more of the following tools while performing the Services (the "CrowdStrike Tools"). CrowdStrike Falcon is not subject to the tools fees as defined in this SOW. Data collected by CrowdStrike Tools is encrypted and stored in the United States or European Union and viewed by personnel in locations that include, but are not limited to, the United States, Canada, United Kingdom, the European Union, New Zealand and Australia.

Falcon Forensics

CrowdStrike personnel may use the Falcon Forensics tool to collect specific data points relevant to the investigation based upon their expertise and knowledge of specific actors/threats. The following are some of the functions performed by Falcon Forensics: directory parsing, handles dump, file hashing, network data dump, detailed process listing, strings extraction, services enumeration, drivers enumeration, environment variables dump, jobs and task enumeration, users and group enumeration.

Falcon Horizon & CrowdStrike Cloud Collectors

CrowdStrike personnel may use Falcon Horizon, a cloud security posture management and detection application, and the CrowdStrike Cloud Collectors, a cloud data collection toolset, to collect and analyze cloud service plane-related information in order to help identify adversary tradecraft and activity.

Falcon Network

CrowdStrike may utilize a threat-specific network monitoring tool referred to as Falcon Network to identify potential outbound malicious communications. CrowdStrike's threat signatures focus on targeted attackers, advanced persistent threats, organized crime and hacktivist groups. Falcon Network is connected to a network egress location and passively captures suspicious traffic in a packet capture library (PCAP). CrowdStrike will not capture any data or signatures other than those necessary to perform the Services. Falcon Network utilizes Corelight and proprietary configurations and tools to maintain a stealth packet capture capability.

CrowdStrike Falcon

CrowdStrike personnel may use CrowdStrike Falcon, a cloud-managed end point detection and response application. CrowdStrike Falcon is comprised of two core components, the cloud-based application and the on-premise device sensor application (Falcon Sensor). CrowdStrike Falcon leverages the lightweight Falcon Sensor that shadows, captures, and correlates low-level operating system events, including, but not limited to: machine event data, executed scripts, code, systems files, log files, DLL files; login data, usernames, binary files, file names, tasks, resource information, commands, protocol identifiers, Internet protocol addresses, URLs, network data, and/or other executable code and metadata. To the extent data collected by the CrowdStrike Tools is aggregated and/or anonymous it is referred to as Execution Profile/Metric Data. Execution Profile/Metric Data, similar to Threat Actor Data, is used for collective security purposes and is not considered Customer Confidential Information. The analysis of the collected data helps identify the adversary tradecraft and activity as opposed to focusing on malware signatures, indicators of compromise, exploits, and vulnerabilities, used in older information security technology. CrowdStrike uses Execution Profile/Metric Data to analyze, characterize, attribute, warn of, and/or respond to threats against you and others, and to analyze trends and to optimize the functionality of CrowdStrike's products and services. CrowdStrike Falcon is equipped with remediation functionality, including but not limited to advanced information gathering (e.g., suspicious or unknown file collection) actions such as executing scripts and executables, deleting a file, terminating processes, and deleting or modifying Windows registry key or value. CrowdStrike provides automatic updates to CrowdStrike Falcon.

Signatures

This SOW may be executed in counterparts, each of which will be considered an original but all of which together will constitute one agreement. Any signature delivered by facsimile or electronic means shall be treated for all purposes as an original. Each of the parties below represents and warrants that the signatory is duly authorized to execute and deliver this SOW and agrees to be bound hereby.

CrowdStrike, Inc.	**NHS Business Services Authority**

By:	Signed via DocuSign on 29/06/2023	By:	Signed via DocuSign on 29/06/2023
Name:		Name:	
Title:		Title:	
Date:		Date:	

Annex 4: CrowdStrike Terms and Conditions

CROWDSTRIKE TERMS AND CONDITIONS

These CrowdStrike Terms and Conditions by and between CrowdStrike, Inc., a Delaware corporation, and any Affiliates performing hereunder (collectively, "**CrowdStrike**") with a principal place of business at 150 Mathilda Place, Suite 300, Sunnyvale, California 94086 and _____ [**Complete with CUSTOMER NAME**], a _____ [**Complete with LEGAL ENTITY AND STATE OR COUNTRY OF ORIGIN**] ("**Customer**"), with a place of business at _____ [**Complete with CUSTOMER STREET ADDRESS, CITY, STATE, COUNTRY AND ZIP CODE**] are entered into as of the date signed by the last party (the "**Effective Date**").

These CrowdStrike Terms and Conditions are a master agreement that cover all CrowdStrike products and services but provisions regarding specific products or services apply only to the extent Customer has purchased, accessed or used such products or services.

1. Definitions.

"**Affiliate**" means any entity that a party directly or indirectly controls (e.g., subsidiary) or is controlled by (e.g., parent), or with which it is under common control (e.g., sibling).

"Agreement" means these CrowdStrike Terms and Conditions together with each Order.

"**API**" means an application program (or programming) interface.

"**CrowdStrike Competitor**" means a person or entity in the business of developing, distributing, or commercializing Internet security products or services substantially similar to or competitive with CrowdStrike's products or services.

"CrowdStrike Data" shall mean the data generated by the CrowdStrike Offerings, including but not limited to, correlative and/or contextual data, and/or detections. For the avoidance of doubt, CrowdStrike Data does not include Customer Data.

"**CrowdStrike Tool**" means any CrowdStrike proprietary software-as-a-service, software, hardware, or other tool that CrowdStrike uses in performing Professional Services, which may be specified in the applicable SOW. CrowdStrike Tools may include CrowdStrike's products.

"**Customer**" means as the context requires, in addition to the entity identified above, any Customer Affiliate that places an Order under these CrowdStrike Terms and Conditions, uses or accesses any Offering hereunder, or benefits from the Customer's use of an Offering.

"Customer Contractor" means any individual or entity (other than a CrowdStrike Competitor) that: (i) has access or use of a Product under this Agreement solely on behalf of and for Customer's Internal Use, (ii) has an agreement to provide Customer (or its Affiliates) services, and (iii) is subject to confidentiality obligations covering CrowdStrike's Confidential Information.

"**Customer Contractor Services**" means products, services or content developed or provided by Customer Contractors, including, but not limited to, third party applications complimentary to the Offerings, implementation services, managed services, training, technical support, or other consulting services related to, or in conjunction with, the Offerings.

"**Documentation**" means CrowdStrike's end-user technical documentation included in the applicable Offering.

"Endpoint" means any physical or virtual device, such as, a computer, server, laptop, desktop computer, mobile, cellular, container or virtual machine image.

"**Error**" means a reproducible failure of a Product to perform in substantial conformity with its applicable Documentation.

"**Internal Use**" means access or use solely for Customer's and subject to the Section entitled *Affiliates, Orders and Payment; Affiliates* and the Section entitled *Access and Use Rights*, its Affiliates', own internal information security purposes. By way of example and not limitation, Internal Use does not include access or use: (i) for the benefit of any person or entity other than Customer or its Affiliates, or (ii) in any event, for the development of any product or service. Internal Use is limited to access and use by Customer's and its Affiliates' employees and Customer Contractors (except as set forth in the Section entitled *Customer Contractors*), in either event, solely on Customer's behalf and for Customer's benefit.

"**Offerings**" means, collectively, any Products, Product-Related Services, or Professional Services.

"**Order**" means any purchase order or other ordering document (including any SOW) accepted by CrowdStrike or a reseller that identifies the following ordered by Customer: Offering, Offering quantity based on CrowdStrike's applicable license metrics (e.g., number of Endpoints, size of company (based on number of employees), number of file uploads, or number of queries), price and Subscription/Order Term.

"**Product**" means any of CrowdStrike's cloud-based software or other products ordered by Customer as set forth in the relevant Order, the available accompanying API's, the CrowdStrike Data, any Documentation and any Updates thereto that may be made available to Customer from time to time by CrowdStrike.

"**Product-Related Services**" means, collectively, (i) Falcon OverWatch, (ii) Falcon Complete Team, (iii) the technical support services for certain Products provided by CrowdStrike, (iv) training, and (v) any other CrowdStrike services provided or sold with Products. Product-Related Services do not include Professional Services.

"**Professional Services**" means any professional services performed by CrowdStrike for Customer pursuant to an SOW or other Order. Professional Services may include without limitation incident response, investigation and forensic services related to cyber-security adversaries, tabletop exercises, and next generation penetration tests related to cyber-security.

2. "Services" means, collectively, any Product-Related Services and any Professional Services.

"**Statement of Work**" or "**SOW**" means a mutually-agreed executed written document describing the Professional Services to be performed by CrowdStrike for Customer, deliverables, fees, and expenses related thereto.

"**Subscription/Order Term**" means the period of time set forth in the applicable Order during which: (i) Customer is authorized by CrowdStrike to access and use the Product or Product-Related Service, or (ii) Professional Services may be performed.

"**Updates**" means any correction, update, upgrade, patch, or other modification or addition made by CrowdStrike to any Product and provided to Customer by CrowdStrike from time to time on an as available basis.

3. Affiliates, Orders and Payment.

3.1 Affiliates. Any Affiliate purchasing hereunder, or using or accessing any Offering hereunder, or benefitting from the Customer's use of an Offering, will be bound by and comply with all terms and conditions of this Agreement. The Customer signing these CrowdStrike Terms and Conditions will remain responsible for Customer's Affiliates' acts and omissions unless Customer's Affiliate has entered into its own Terms and Conditions with CrowdStrike.

3.2 Orders. Only those transaction-specific terms stating the Offerings ordered, quantity, price, payment terms, Subscription/Order Term, and billing/provisioning contact information (and for the avoidance of doubt, specifically excluding any pre-printed terms on a Customer or reseller purchase order) will have any force or effect unless a particular Order is executed by an authorized signer of CrowdStrike and returned to Customer (or the applicable reseller). If any such Order is so executed and delivered, then only those specific terms on the face of such Order that expressly identify those portions of this Agreement that are to be superseded will prevail over any conflicting terms herein but only with respect to those Offerings ordered on such Order. Orders are non-cancellable. Any Order through a reseller is subject to, and CrowdStrike's obligations and liabilities to Customer are governed by, this Agreement.

3.3 Payment and Taxes. Customer will pay the fees for Offerings to a reseller or CrowdStrike as set forth in the applicable Order. Unless otherwise expressly set forth on the Order, Customer will pay the fees and amounts stated on each Order within 30 days after receipt of the applicable invoice. Except as otherwise expressly provided in this Agreement, all fees and other amounts are non-refundable. Fees are exclusive of any applicable sales, use, value added, withholding, and other taxes, however designated. Customer shall pay all such taxes levied or imposed by reason of Customer's purchase of the Offerings and the transactions hereunder, except for taxes based on CrowdStrike's income or with respect to CrowdStrike's employment of its employees.

4. Access & Use Rights.

4.1 Evaluation. If CrowdStrike approves Customer's evaluation use of a CrowdStrike product ("**Evaluation Product**"), the terms herein applicable to Products also apply to evaluation access and use of such Evaluation Product, except for the following different or additional terms: (i) the duration of the evaluation is as mutually agreed upon by Customer and CrowdStrike, provided, that either CrowdStrike or Customer can terminate the evaluation at any time upon written (including email) notice to the other party; (ii) the Evaluation Product is provided "AS-IS" without warranty of any kind, and CrowdStrike disclaims all warranties, support obligations, and other liabilities and obligations for the Evaluation Product; and (iii) Customer's access and use is limited to Internal Use by Customer employees only.

4.2 Access & Use Rights. Subject to the terms and conditions of this Agreement (including CrowdStrike's receipt of applicable fees), CrowdStrike grants Customer, under CrowdStrike's intellectual property rights in and to the applicable Product, a non-exclusive, non-transferable (except as expressly provided in the Section entitled *Assignment*), non-sublicensable license to access and use the Products in accordance with any applicable Documentation solely for Customer's Internal Use during the applicable Subscription/Order Term. Customer's access and use is limited to the quantity in the applicable Order. Furthermore, the following additional terms and conditions apply to specific Products (or components thereof):

(a) Products with Software Components. If Customer purchases a subscription to a Product with a downloadable object-code component ("**Software Component**"), Customer may, during the Subscription/Order Term install and run multiple copies of the Software Components solely for Customer's and Customer's Affiliates' Internal Use up to the maximum quantity in the applicable Order.

(b) CrowdStrike Tools. If CrowdStrike provides CrowdStrike Tools to Customer pursuant to performing Professional Services, the license set forth in the Section entitled *Access & Use Rights* applies to such CrowdStrike Tools as used solely for Customer's Internal Use during the period of time set forth in the applicable Order, or if none is specified, for the period authorized by CrowdStrike. Not all Professional Services engagements will involve the use of CrowdStrike Tools.

4.3 Restrictions. The access and use rights set forth in the Section entitled *Access & Use Rights* do not include any rights to, and Customer will not, with respect to any Offering (or any portion thereof): (i) employ or authorize a CrowdStrike Competitor to use or view the Offering or Documentation, or to provide management, hosting, or support for an Offering; (ii) alter, publicly display, translate, create derivative works of or otherwise modify an Offering; (iii) sublicense, distribute or otherwise transfer an Offering to any third party (except as expressly provided in the Section entitled *Assignment*); (iv) allow third parties to access or use an Offering (except for Customer Contractors as expressly permitted herein); (v) create public Internet "links" to an Offering or "frame" or "mirror" any Offering content on any other server or wireless or Internet-based device; (vi) reverse engineer, decompile, disassemble or otherwise attempt to derive the source code (if any) for an Offering (except to the extent that such prohibition is expressly precluded by applicable law), circumvent its functions, or attempt to gain unauthorized access to an Offering or its related systems or networks; (vii) use an Offering to circumvent the security of another party's network/information, develop malware, unauthorized surreptitious surveillance, data modification, data exfiltration, data ransom or data destruction; (viii) remove or alter any notice of proprietary right appearing on an Offering; (ix) conduct any stress tests, competitive benchmarking or analysis on, or publish any performance data of, an Offering (provided, that this does not prevent Customer from comparing the Products to other products for Customer's Internal Use); (x) use any feature of CrowdStrike APIs for any purpose other than in the performance of, and in accordance with, this Agreement; or (xi) cause, encourage or assist any third party to do any of the foregoing. Customer agrees to use an Offering in accordance with laws, rules and regulations directly applicable to Customer and acknowledges that Customer is solely responsible for determining whether a particular use of an Offering is compliant with such laws.

4.4 Installation and User Accounts. CrowdStrike is not responsible for installing Products unless Customer purchases installation services from CrowdStrike. For those Products requiring user accounts, only the single individual user assigned to a user account may access or use the Product. Customer is liable and responsible for all actions and omissions occurring under Customer's and Customer Contractor's user accounts for Offerings. Customer shall notify CrowdStrike if Customer learns of any unauthorized access or use of Customer's user accounts or passwords for an Offering.

4.5 Malware Samples. If CrowdStrike makes malware samples available to Customer in connection with an evaluation or use of the Product ("**Malware Samples**"), Customer acknowledges and agrees that: (i) Customer's access to and use of Malware Samples is at Customer's own risk, and (ii) Customer should not download or access any Malware Samples on or through its own production systems and networks and that doing so can infect and damage Customer's systems, networks, and data. Customer shall use the Malware Samples solely for Internal Use and not for any malicious or unlawful purpose. CrowdStrike will not be liable for any loss or damage caused by any Malware Sample that may infect Customer's computer equipment, computer programs, data, or other proprietary material due to Customer's access to or use of the Malware Samples.

4.6 Third Party Software. CrowdStrike uses certain third party software in its Products, including what is commonly referred to as open source software. Under some of these third party licenses, CrowdStrike is required to provide Customer with notice of the license terms and attribution to the third party. See the licensing terms and attributions for such third party software that CrowdStrike uses at: https://falcon.crowdstrike.com/opensource.

4.7 Ownership & Feedback. Products, Product-Related Services and the CrowdStrike Tools are made available for use or licensed, not sold. CrowdStrike owns and retains all right, title and interest (including all intellectual property rights) in and to the Products, Product-Related Services and the CrowdStrike Tools. Any feedback or suggestions that Customer provides to CrowdStrike regarding its Offerings and CrowdStrike Tools (e.g., bug fixes and features requests) is non-confidential and may be used by CrowdStrike for any purpose without acknowledgement or compensation; provided, Customer will not be identified publicly as the source of the feedback or suggestion.

5. Customer Contractors.

5.1 Authorization. Customer authorizes CrowdStrike to give Customer Contractors the rights and privileges to the Offerings necessary to enable and provide for Customer's use and receipt of the Customer Contractor Services. If at any time Customer revokes this authorization, to the extent the Offerings provide for Customer to limit the Customer Contractor's access and use of the Offerings, then Customer is responsible for taking the actions necessary to revoke such access and use. In the event Customer requires CrowdStrike assistance with such revocation or limitation, Customer must contact CrowdStrike Support with written notice of such revocation or limitation at support@crowdstrike.com and CrowdStrike will disable the Customer Contractor's access to Customer's Offerings within a reasonable period of time following receipt of such notice but in any event within 72 hours of receipt of such notice.

5.2 Disclaimer. Customer Contractors are subject to the terms and conditions in the Agreement while they are using the Offerings on behalf of Customer and Customer remains responsible for their acts and omissions during such time. Any breach by a Customer Contractor of this Agreement is a breach by Customer. CrowdStrike may make available Customer Contractor Services to Customer, for example, through an online directory, catalog, store, or marketplace. Customer Contractor Services are not required for use of the Offerings. Offerings may contain features, including API's, designed to interface with or provide data to Customer Contractor Services. CrowdStrike is not responsible or liable for any loss, costs or damages arising out of Customer Contractor's actions or inactions in any manner, including but not limited to, for any disclosure, transfer, modification or deletion of Customer Data (defined in Exhibit A). Whether or not a Customer Contractor is designated by CrowdStrike as, or otherwise claims to be "certified," "authorized," or similarly labeled, CrowdStrike does not: (i) control, monitor, maintain or provide support for, Customer Contractor Services, (ii) disclaims all warranties of any kind, indemnities, obligations, and other liabilities in connection with the Customer Contractor Services, and any Customer Contractor interface or integration with the Offerings, and (iii) cannot guarantee the continued availability of Customer Contractor Services and related features. If Customer Contractor Services and related features are no longer available for any reason, CrowdStrike is not obligated to provide any refund, credit, or other compensation for, or related to, the Offerings.

5.3 Restrictions on Customer Contractors. Customer shall not give or allow Customer Contractors access to, or use of, intelligence reports provided by, or made accessible in, the Products. For the avoidance of doubt, nothing herein prevents Customer from using intelligence API's in Customer Contractor Services for Customer's Internal Use.

6. Professional Services.

6.1 Fees. Professional Services will commence on a mutually agreed upon date. Estimates provided for Professional Services performed on a time-and-material basis are estimates only and not a guaranteed time of completion. Professional Services performed on a fixed fee basis are limited to the scope of services stated in the applicable Order.

6.2 Ownership of Deliverables. Professional Services do not constitute "works for hire," "works made in the course of duty," or similar terms under laws where the transfer of intellectual property occurs on the performance of services to a payor. The only deliverable arising from the Professional Services is a report consisting primarily of CrowdStrike's findings, recommendations, and adversary information. Customer owns the copy of the report (including without limitation, all of Customer's Confidential Information therein) delivered to Customer ("**Deliverable**"), subject to CrowdStrike's ownership of the CrowdStrike Materials. Customer agrees that relative to Customer, CrowdStrike exclusively owns any and all software (including object and source code), flow charts, algorithms, documentation, adversary information, report templates, know-how, inventions, techniques, models, CrowdStrike trademarks, ideas and any and all other works and materials developed by CrowdStrike in connection with performing the Professional Services (including without limitation all intellectual property rights therein and thereto) (collectively, the "**CrowdStrike Materials**") and that title shall remain with CrowdStrike. For the avoidance of doubt, the CrowdStrike Materials do not include any Customer Confidential Information or other Customer provided materials or data. Upon payment in full of the amounts due hereunder for the applicable Professional Services and to the extent the CrowdStrike Materials are incorporated into the Deliverable(s), Customer shall have a perpetual, non-transferable (except as expressly provided in the Section entitled *Assignment*), non-exclusive license to use the CrowdStrike Materials solely as a part of the Deliverable(s) for Customer's Internal Use.

7. Data Security and Privacy. See Exhibit A.

8. Confidentiality.

8.1 Definitions. In connection with this Agreement, each party ("**Recipient**") may receive Confidential Information of the other party ("**Discloser**") or third parties to whom Discloser has a duty of confidentiality. "**Confidential Information**" means non-public information in any form that is in the Recipient's possession regardless of the method of acquisition that the Discloser designates as confidential to Recipient or should be reasonably known by the Recipient to be Confidential Information due to the nature of the information disclosed and/or the circumstances surrounding the disclosure. Confidential Information shall not include information that is: (i) in or becomes part of the public domain (other than by disclosure by Recipient in violation of this Agreement); (ii) previously known to Recipient without an obligation of confidentiality and demonstrable by the Recipient; (iii) independently developed by Recipient without use of Discloser's Confidential Information; or (iv) rightfully obtained by Recipient from third parties without an obligation of confidentiality.

8.2 Restrictions on Use. Except as allowed in Section 7.3 (*Exceptions*), Recipient shall hold Discloser's Confidential Information in strict confidence and shall not disclose any such Confidential Information to any third party, other than to its employees, and contractors, including without limitation, counsel, accountants, and financial advisors (collectively, "Representatives"), its Affiliates and their Representatives, subject to the other terms of this Agreement, and in each case who need to know such information and who are bound by restrictions regarding disclosure and use of such information comparable to and no less restrictive than those set forth herein. Recipient shall not use Discloser's Confidential Information for any purpose other than as set forth in this Agreement. Recipient shall take the same degree of care that it uses to protect its own confidential information of a similar nature and importance (but in no event less than reasonable care) to protect the confidentiality and avoid the unauthorized use, disclosure, publication, or dissemination of the Discloser's Confidential Information. Within 72 hours of Recipient becoming aware of the unauthorized use, disclosure, publication, or dissemination of the Discloser's Confidential Information while in Recipient's control, Recipient shall provide Discloser with notice thereof.

8.3 Exceptions. Recipient may disclose Discloser's Confidential Information: (i) to the extent required by applicable law or regulation; (ii) pursuant to a subpoena or order of a court or regulatory, self-regulatory, or legislative body of competent jurisdiction; (iii) in connection with any regulatory report, audit, or inquiry; or (iv) where requested by a regulator with jurisdiction over Recipient. In the event of such a requirement or request, Recipient shall, to the extent legally permitted: (a) give Discloser prompt written notice of such requirement or request prior to such disclosure; and (b) at Discloser's cost, a reasonable opportunity to review and comment upon the disclosure and request confidential treatment or a protective order pertaining thereto prior to Recipient making such disclosure. If the Recipient is legally required to disclose the Discloser's Confidential Information as part of: (x) a legal proceeding to which the Discloser is a party but the Recipient is not; or (y) a government or regulatory investigation of the Discloser, the Discloser shall pay all of the Recipient's reasonable and actual out of pocket legal fees and expenses (as evidenced by reasonably detailed invoices) and will reimburse the Recipient for its reasonable costs and fees of compiling and providing such Confidential Information, including, a reasonable hourly rate for time spent preparing for, and participating in, depositions and other testimony.

8.4 Destruction. Upon Discloser's written request, Recipient shall use commercially reasonable efforts to destroy the Confidential Information and any copies or extracts thereof. However, Recipient, its Affiliates and their Representatives may retain any Confidential Information that: (i) they are required to keep for compliance purposes under a document retention policy or as required by applicable law, professional standards, a court, or regulatory agency; or (ii) have been created electronically pursuant to automatic or ordinary course archiving, back-up, security, or disaster recovery systems or procedures; provided, however, that any such retained information shall remain subject to this Agreement. Upon Discloser's request, Recipient will provide Discloser with written confirmation of destruction in compliance with this provision.

8.5 Equitable Relief. Each party acknowledges that a breach of this Section 7 (*Confidentiality*) shall cause the other party irreparable injury and damage. Therefore, each party agrees that those breaches may be stopped through injunctive proceedings in addition to any other rights and remedies which may be available to the injured party at law or in equity without the posting of a bond.

9. Warranties & Disclaimer.

9.1 No Warranty for Pre-Production Versions. Any pre-production feature or version of an Offering provided to Customer is *experimental* and provided "AS IS" without warranty of any kind and will not create any obligation for CrowdStrike to continue to develop, productize, support, repair, offer for sale, or in any other way continue to provide or develop any such feature or Offering. Customer agrees that its purchase is not contingent on the delivery of any future functionality or features, or dependent on any oral or written statements made by CrowdStrike regarding future functionality or features.

9.2 Product Warranty. If Customer has purchased a Product, CrowdStrike warrants to Customer during the applicable Subscription/Order Term that: (i) the Product will operate without Error; and (ii) CrowdStrike has used industry standard techniques to prevent the Products at the time of delivery from injecting malicious software viruses into Customer's Endpoints where the Products are installed. Customer must notify CrowdStrike of any warranty claim during the Subscription/Order Term. Customer's sole and exclusive remedy and the entire liability of CrowdStrike for its breach of this warranty will be for CrowdStrike, at its own expense to do at least one of the following: (a) use commercially reasonable efforts to provide a work-around or correct such Error; or (b) terminate Customer's license to access and use the applicable non-conforming Product and refund the prepaid fee prorated for the unused period of the Subscription/Order Term. CrowdStrike shall have no obligation regarding Errors reported after the applicable Subscription/Order Term.

9.3 Services Warranty. CrowdStrike warrants to Customer that it will perform all Services in a professional and workmanlike manner consistent with generally accepted industry standards. Customer must notify CrowdStrike of any warranty claim for Services during the period the Services are being performed or within 30 days after the conclusion of the Services. Customer's sole and exclusive remedy and the entire liability of CrowdStrike for its breach of this warranty will be for CrowdStrike, at its option and expense, to (a) use commercially reasonable efforts to re-perform the non-conforming Services, or (b) refund the portion of the fees paid attributable to the non-conforming Services.

9.4 Exclusions. The express warranties do not apply if the applicable Product or Service: (i) has been modified, except by CrowdStrike, (ii) has not been installed, used, or maintained in accordance with this Agreement or

Documentation, or (iii) is non-conforming due to a failure to use an applicable Update. If any part of a Product or Service references websites, hypertext links, network addresses, or other third party locations, information, or activities, it is provided as a convenience only.

9.5 No Guarantee. CUSTOMER ACKNOWLEDGES, UNDERSTANDS, AND AGREES THAT CROWDSTRIKE DOES NOT GUARANTEE OR WARRANT THAT IT WILL FIND, LOCATE, OR DISCOVER ALL OF CUSTOMER'S OR ITS AFFILIATES' SYSTEM THREATS, VULNERABILITIES, MALWARE, AND MALICIOUS SOFTWARE, AND CUSTOMER AND ITS AFFILIATES WILL NOT HOLD CROWDSTRIKE RESPONSIBLE THEREFOR.

9.6 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES IN THIS SECTION 8, CROWDSTRIKE AND ITS AFFILIATES DISCLAIM ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CROWDSTRIKE AND ITS AFFILIATES AND SUPPLIERS SPECIFICALLY DISCLAIM ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGMENT WITH RESPECT TO THE OFFERINGS AND CROWDSTRIKE TOOLS. THERE IS NO WARRANTY THAT THE OFFERINGS OR CROWDSTRIKE TOOLS WILL BE ERROR FREE, OR THAT THEY WILL OPERATE WITHOUT INTERRUPTION OR WILL FULFILL ANY OF CUSTOMER'S PARTICULAR PURPOSES OR NEEDS. THE OFFERINGS AND CROWDSTRIKE TOOLS ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. NEITHER THE OFFERINGS NOR CROWDSTRIKE TOOLS ARE FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY, OR PROPERTY DAMAGE. Customer agrees that it is Customer's responsibility to ensure safe use of an Offering and the CrowdStrike Tools in such applications and installations. CROWDSTRIKE DOES NOT WARRANT ANY THIRD PARTY PRODUCTS OR SERVICES.

8.7 Additional Terms That May Apply. See Exhibit C for additional warranties that may apply to certain Customers.

10. Indemnification.

10.1 CrowdStrike's Obligation. CrowdStrike shall at its cost and expense: (i) defend and/or settle any claim brought against Customer by an unaffiliated third party alleging that an Offering infringes or violates that third party's intellectual property rights, and (ii) pay and indemnify any settlement of such claim or any damages awarded to such third party by a court of competent jurisdiction as a result of such claim; provided, that Customer: (a) gives CrowdStrike prompt written notice of such claim; (b) permits CrowdStrike to solely control and direct the defense or settlement of such claim (however, CrowdStrike will not settle any claim in a manner that requires Customer to admit liability without Customer's prior written consent); and (c) provides CrowdStrike all reasonable assistance in connection with the defense or settlement of such claim, at CrowdStrike's cost and expense. In addition, Customer may, at Customer's own expense, participate in defense of any claim.

10.2 Remedies. If a claim covered under this Section occurs or in CrowdStrike's opinion is reasonably likely to occur, CrowdStrike may at its expense and sole discretion (and if Customer's access and use of an Offering is enjoined, CrowdStrike will, at its expense): (i) procure the right to allow Customer to continue using the applicable Offering; (ii) modify or replace the applicable Offering to become non-infringing; or (iii) if neither (i) nor (ii) is commercially practicable, terminate Customer's license or access to the affected portion of applicable Offering and refund a portion of the pre-paid, unused fees paid by Customer corresponding to the unused period of the Subscription/Order Term.

10.3 Exclusions. CrowdStrike shall have no obligations under this Section if the claim is based upon or arises out of: (i) any modification to the applicable Offering not made by CrowdStrike; (ii) any combination or use of the applicable Offering with or in any third party software, hardware, process, firmware, or data, to the extent that such claim is based on such combination or use; (iii) Customer's continued use of the allegedly infringing Offering after being notified of the infringement claim or after being provided a modified version of the Offering by CrowdStrike at no additional cost that is intended to address such alleged infringement; (iv) Customer's failure to use the Offering in accordance with the applicable Documentation; and/or (v) Customer's use of the Offering outside the scope of the rights granted under this Agreement.

10.4 Exclusive Remedy. THE REMEDIES SPECIFIED IN THIS SECTION CONSTITUTE CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES, AND CROWDSTRIKE'S ENTIRE LIABILITY, WITH RESPECT TO ANY INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

11. Limitation of Liability.

11.1 TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT FOR LIABILITY FOR ANY AMOUNTS PAID OR PAYABLE TO THIRD PARTIES UNDER SECTION 9 (*INDEMNIFICATION*), CUSTOMER'S PAYMENT OBLIGATIONS, AND/OR ANY INFRINGEMENT OR MISAPPROPRIATION BY ONE PARTY OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY IN CONNECTION WITH THIS AGREEMENT OR THE SUBJECT MATTER HEREOF (UNDER ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STATUTE, TORT OR OTHERWISE) FOR ANY LOST PROFITS, REVENUE, OR SAVINGS, LOST BUSINESS OPPORTUNITIES, LOST DATA, OR SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES OR SUCH DAMAGES OR LOSSES WERE REASONABLY FORESEEABLE; OR (B) AN AMOUNT THAT EXCEEDS THE TOTAL FEES PAID OR PAYABLE TO CROWDSTRIKE FOR THE RELEVANT OFFERING DURING THAT OFFERING'S SUBSCRIPTION/ORDER TERM. THESE LIMITATIONS WILL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY REMEDY SPECIFIED IN THIS AGREEMENT. MULTIPLE CLAIMS SHALL NOT EXPAND THE LIMITATIONS SPECIFIED IN THIS SECTION 10.

11.2 Additional or Different Terms That May Apply. See Exhibit C for additional or different terms related to liability that may apply to certain Customers.

12. Compliance with Laws. Each party agrees to comply with all U.S. federal, state, local and non-U.S. laws directly applicable to such party in the performance of this Agreement, including but not limited to, applicable export and import, anti-corruption and employment laws. Customer acknowledges and agrees the Offerings shall not be used, transferred, or otherwise exported or re-exported to regions that the United States and/or the European Union maintains an embargo or comprehensive sanctions (collectively, "Embargoed Countries"), or to or by a national or resident thereof, or any person or entity subject to individual prohibitions (e.g., parties listed on the U.S. Department of Treasury's List of Specially Designated Nationals or the U.S. Department of Commerce's Table of Denial Orders) (collectively, "Designated Nationals"), without first obtaining all required authorizations from the U.S. government and any other applicable government. Customer represents and warrants that Customer is not located in, or is under the control of, or a national or resident of, an Embargoed Country or Designated National. CrowdStrike represents and warrants that CrowdStrike is not located in, or is under the control of, or a national or resident of, an Embargoed Country or Designated National.

13. U.S. Government End Users.

13.1 Commercial Items. The following applies to all acquisitions by or for the U.S. government or by any U.S Government prime contractor or subcontractor at any tier ("Government Users") under any U.S. Government contract, grant, other transaction, or other funding agreement. The Products, CrowdStrike Tools, and Documentation are "commercial items," as that term is defined in Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in FAR 12.211 and 12.212. In addition, Department of Defense FAR Supplement ("DFARS") 252.227-7015 (Technical Data – Commercial Items) applies to technical data acquired by Department of Defense agencies. Consistent with FAR 12.211 and 12.212 and DFARS (48 C.F.R.) 227.7202-1 through 227.7202-4, the Products, CrowdStrike Tools, and Documentation are being licensed to Government Users pursuant to the terms of this license(s) customarily provided to the public as forth in this Agreement, unless such terms are inconsistent with United States federal law ("Federal Law").

13.2 Disputes with the U.S. Government. If this Agreement fails to meet the Government's needs or is inconsistent in any way with Federal Law and the parties cannot reach a mutual agreement on terms for this Agreement, the Government agrees to terminate its use of the Offerings. In the event of any disputes with the U.S. Government in connection with this Agreement, Section 14.3 of this Agreement shall not apply. Instead the rights and duties of the parties arising from this Agreement, shall be governed by, construed, and enforced in accordance with Federal Procurement Law and any such disputes shall be resolved pursuant to the Contract Disputes Act of 1978, as amended (41 U.S.C. 7101-7109), as implemented by the Disputes Clause, FAR 52.233-1.

12.3 Precedence. This U.S. Government rights in this Section are in lieu of, and supersedes, any other FAR, DFARS, or other clause, provision, or supplemental regulation that addresses Government rights in the Offerings, computer software or technical data under this Agreement.

14. Suspension and Termination. This Agreement shall remain effective until termination in accordance with this Section or as otherwise specified herein. CrowdStrike may immediately suspend Customer's access to, or use of, the Offerings if: (i) CrowdStrike believes that there is a significant threat to the security, integrity, functionality, or availability of the Offerings or any content, data, or applications in the Offerings; (ii) Customer or Customer users are in breach of Section 3.3 (*Restrictions*); or (iii) Customer fails to pay CrowdStrike when undisputed fees are due; provided, however, CrowdStrike will use commercially reasonable efforts under the circumstances to provide Customer with notice and, if applicable, an opportunity to remedy such violation prior to any such suspension. Either party may terminate this Agreement upon 30 days' written notice of a material breach by the other party, unless the breach is cured within the 30-day notice period. Prior to termination and subject to the terms of this Agreement, Customer shall have the right to access and download Customer Data available per the Customer's purchased Products and data retention period in a manner and in a format supported by the Products. Upon termination of this Agreement for any reason: (a) all Customer's access and use rights granted in this Agreement will terminate; (b) Customer must promptly cease all use of Offerings and de-install all Software Components installed on Customer's Endpoints; and (c) Customer Data will be deleted in accordance with the data retention period purchased by Customer and Section 7.4 *Confidentiality; Destruction*). Sections 1, 3.3, 7, 10, 12, 13, and 14 and all liabilities that accrue prior to termination shall survive expiration or termination of this Agreement for any reason.

15. General.

15.1 Entire Agreement. This Agreement constitutes the entire agreement between Customer and CrowdStrike concerning the subject matter of this Agreement and it supersedes all prior and simultaneous proposals, agreements, understandings, or other communications between the parties, oral or written, regarding such subject matter. Notwithstanding the foregoing, if you have a CrowdStrike *Limited Warranty Agreement for Falcon Complete* (or a preceding or successor named product) fully executed with CrowdStrike, the warranty provided therein stands alone and is not superseded by this Agreement. It is expressly agreed that the terms of this Agreement shall supersede any terms in any procurement Internet portal or other similar non-CrowdStrike document and no such terms included in any such portal or other non-CrowdStrike document shall apply to the Offerings ordered. Any Order through a reseller is subject to, and CrowdStrike's obligations and liabilities to Customer are governed by, this Agreement. CrowdStrike is not obligated under any reseller's agreement with you unless an officer of CrowdStrike executes the agreement. This Agreement shall not be construed for or against any party to this Agreement because that party or that party's legal representative drafted any of its provisions.

15.2 Assignment. Neither party may assign this Agreement without the prior written consent of the other party, except to an Affiliate in connection with a corporate reorganization or in connection with a merger, acquisition, or sale of all or substantially all of its business and/or assets. Any assignment in violation of this Section shall be void. Subject to the foregoing, all rights and obligations of the parties under this Agreement shall be binding upon and inure to the benefit of and be enforceable by and against the successors and permitted assigns.

15.3 Governing Law; Venue. Except as otherwise provided in Exhibit B (if applicable), this Agreement, and the rights and duties of the parties arising from this Agreement, shall be governed by, construed, and enforced in accordance with the laws of the State of California, excluding its conflicts-of-law principles. The sole and exclusive jurisdiction and venue for actions arising under this Agreement shall be state and federal courts in Santa Clara County, California, and the parties agree to service of process in accordance with the rules of such courts. The Uniform Computer Information Transactions Act and the United Nations Convention on the International Sale of Goods shall not apply. Notwithstanding the foregoing, each party reserves the right to file a suit or action in any court of competent jurisdiction as such party deems necessary to protect its intellectual property rights and, in CrowdStrike's case, to recoup any payments due.

15.4 Independent Contractors; No Third Party Rights. The parties are independent contractors. This Agreement shall not establish any relationship of partnership, joint venture, employment, franchise, or agency between the parties. No provision in this Agreement is intended or shall create any rights with respect to the subject matter of this Agreement in any third party.

15.5 Waiver, Severability & Amendments. The failure of either party to enforce any provision of this Agreement shall not constitute a waiver of any other provision or any subsequent breach. If any provision of this Agreement is held to be illegal, invalid, or unenforceable, the provision will be enforced to the maximum extent permissible so as to affect the intent of the parties, and the remaining provisions of this Agreement will remain in full force and effect. This Agreement may only be amended, or any term or condition set forth herein waived, by written consent of both parties.

15.6 Force Majeure. Neither party shall be liable for, nor shall either party be considered in breach of this Agreement due to, any failure to perform its obligations under this Agreement (other than its payment obligations) as a result of a cause beyond its control, including but not limited to, act of God or a public enemy, act of any military, civil or regulatory authority, change in any law or regulation, fire, flood, earthquake, storm or other like event, disruption or outage of communications (including an upstream server block and Internet or other networked environment disruption or outage), power or other utility, labor problem, or any other cause, whether similar or dissimilar to any of the foregoing, which could not have been prevented with reasonable care. The party experiencing a force majeure event, shall use commercially reasonable efforts to provide notice of such to the other party.

15.7 Notices. All legal notices will be given in writing to the addresses in the first introductory paragraph of this Agreement and will be effective: (i) when personally delivered, (ii) on the reported delivery date if sent by a recognized international or overnight courier, or (iii) five business days after being sent by registered or certified mail (or ten days for international mail). For clarity, Orders, POs, confirmations, invoices, and other documents relating to order processing and payment are not legal notices and may be delivered electronically in accordance with each party's standard ordering procedures.

15.8 Signatures. This Agreement and any Orders may be executed in two counterparts, each of which will be considered an original but all of which together will constitute one agreement. Any signature delivered by electronic means shall be treated for all purposes as an original.

16.	**CROWDSTRIKE, INC.**	**LEGAL NAME OF CUSTOMER:**
17.		
18.	_____	
19.		
20.	**By:** _____	**By:** _____
21.		
22.	**Name:** _____	**Name:** _____
23.		
24.	**Title:** _____	**Title:** _____
25.		
26.	**Date:** _____	**Date:** _____

Exhibit A: Data Security and Privacy Schedule

1. **Definitions**
   a. **"CrowdStrike Systems"** means those computer systems hosting the 'Falcon EPP Platform'.
   b. **"Customer Data"** means the data generated by the Customer's Endpoint and collected by: (i) the Products, and/or (ii) the CrowdStrike Tools, and in either case, sent to the CrowdStrike Systems. Customer Data is considered Customer's Confidential Information (defined in Section 7 *Confidentiality*) and subject to the exclusions, exceptions and obligations set forth therein and this Exhibit A *Data Security and Privacy Schedule*.
   c. **"Execution Profile/Metric Data"** means any machine-generated data, such as metadata derived from tasks, file execution, commands, resources, network telemetry, executable binary files, macros, scripts, and processes, that: (i) Customer provides to CrowdStrike in connection with this Agreement or (ii) is collected or discovered during the course of CrowdStrike providing Offerings, excluding any such information or data that identifies Customer or to the extent it includes Personal Data.
   d. **"Personal Data"** means information provided by Customer to CrowdStrike or collected by CrowdStrike from Customer used to distinguish or trace a natural person's identity, either alone or when combined with other personal or identifying information that is linked or linkable by CrowdStrike to a specific natural person. Personal Data also includes such other information about a specific natural person to the extent that the data protection laws applicable in the jurisdictions in which such person resides define such information as Personal Data.
   e. **"Privacy and Security Laws"** means U.S. federal, state and local and non-U.S. laws, including those of the European Union, that regulate the privacy or security of Personal Data and that are directly applicable to CrowdStrike.
   f. **"Security Breach"** means unauthorized access to, or unauthorized acquisition of: (i) Customer Data, or (ii) Personal Data, stored on CrowdStrike Systems that results in the compromise of such Customer Data and/or Personal Data.
   g. **"Threat Actor Data"** means any malware, spyware, virus, worm, Trojan horse, or other potentially malicious or harmful code or files, URLs, DNS data, network telemetry, commands, processes or techniques, metadata, or other information or data, in each case that is potentially related to unauthorized third parties associated therewith and that: (i) Customer provides to CrowdStrike in connection with this Agreement, or (ii) is collected or discovered during the course of CrowdStrike providing Offerings, excluding any such information or data that identifies Customer or to the extent that it includes Personal Data.

2. **Falcon Platform**
   The 'Falcon EPP Platform' uses a crowd-sourced environment, for the benefit of all customers, to help customers protect themselves against suspicious and potentially destructive activities. CrowdStrike's Products are designed to detect, prevent, respond to, and identify intrusions by collecting and analyzing data, including machine event data, executed scripts, code, system files, log files, dll files, login data, binary files, tasks, resource information, commands, protocol identifiers, URLs, network data, and/or other executable code and metadata. Customer, rather than CrowdStrike, determines which types of data, whether Personal Data or not, exist on its systems. Accordingly, Customer's endpoint environment is unique in configurations and naming conventions and the machine event data could potentially include Personal Data. CrowdStrike uses the data to: (i) analyze, characterize, attribute, warn of, and/or respond to threats against Customer and other customer, (ii) analyze trends and performance, (iii) improve the functionality of, and develop, CrowdStrike's products and services, and enhance cybersecurity; and (iv) permit Customers to leverage other applications that use the data, but for all of the foregoing, in a way that does not identify Customer or Customer's Personal Data to other customers. Neither Execution Profile/Metric Data nor Threat Actor Data are Customer's Confidential Information or Customer Data.

3. **Processing Personal Data**
   a. Provisioning/Use of Offerings**.** Personal Data may be collected and used during the provisioning and use of the Offerings to deliver, support and improve the Offerings, administer the Agreement and further the business relationship between Customer and CrowdStrike, comply with law, act in accordance with Customer's written instructions, or otherwise in accordance with this Agreement. Customer authorizes CrowdStrike to collect, use, store, and transfer the Personal Data that Customer provides to CrowdStrike as contemplated in this Agreement.

b. Suspicious/Unknown File Analysis. While using certain CrowdStrike Offerings Customer may have the option to upload (by submission, configuration, and/or, in the case of Services, by CrowdStrike personnel retrieval) files and other information related to the files for security analysis and response or, when submitting crash reports, to make the product more reliable and/or improve CrowdStrike's products and services or enhance cyber-security. These potentially suspicious or unknown files may be transmitted and analyzed to determine functionality and their potential to cause instability or damage to Customer's endpoints and systems. In some instances, these files could contain Personal Data for which Customer is responsible.

4. Compliance with Privacy and Information Security Requirements

a. Compliance with Laws. CrowdStrike shall comply with all Privacy and Security Laws, the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of Personal Data from the European Economic Area, Switzerland, and the United Kingdom, as applicable. CrowdStrike's privacy notice may be found at http://www.crowdstrike.com/privacy-notice/. To the extent necessary to comply with Privacy and Security Laws, including but not limited to when Customer is a controller of Personal Data processed by CrowdStrike originating in the European Union, Switzerland, or the United Kingdom, the Data Protection Addendum set forth here https://www.crowdstrike.com/data-protection-agreement/ shall apply to CrowdStrike's processing of such Customer Personal Data.

b. Safeguards. CrowdStrike shall maintain appropriate technical and organizational safeguards commensurate with the sensitivity of the Customer Data and Personal Data processed by it on Customer's behalf, which are designed to protect the security, confidentiality, and integrity of such Customer Data and Personal Data and protect such Customer Data and Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, including the safeguards set forth on Appendix 1 which substantially conform to the ISO/IEC 27002 control framework. ("Information Security Controls for CrowdStrike Systems").

c. Access; Contacts. With respect to employees, agents, and subcontractors, CrowdStrike shall limit access to Customer Data and Personal Data to only those employees, agents, and subcontractors who have a need to access the Customer Data and/or Personal Data in order to carry out their roles as contemplated in the terms of this Agreement. CrowdStrike shall assign and train personnel who shall: (i) liaise with customers regarding any issues concerning the security of Customer Data and/or Personal Data; (ii) receive notice of any Security Breach discovered by CrowdStrike and provide notice of any such Security Breach to Customer; and (iii) coordinate CrowdStrike's Security Breach response and remedial action.

5. Security Breach Response

In the event CrowdStrike discovers a Security Breach, CrowdStrike shall:

a. Without undue delay but no later than 72 hours of becoming aware, notify Customer of the discovery of the Security Breach. Such notice shall summarize the known circumstances of the Security Breach and the corrective action taken or to be taken by CrowdStrike.

b. Conduct an investigation of the circumstances of the Security Breach.

c. Use commercially reasonable efforts to remediate the Security Breach.

d. Use commercially reasonable efforts to communicate and cooperate with Customer concerning its response to the Security Breach.

6. Security Assessment and Provision of Audited Security Controls. Promptly after written (including email) request from Customer, CrowdStrike shall provide Customer with: (i) its most recent SOC II, Type 2 report regarding the CrowdStrike Systems; and (ii) provide its completed Standardized Information Gathering (SIG) questionnaire (or similar document) for the CrowdStrike Systems (the "Security Documentation"). Upon the provision of reasonable notice to CrowdStrike, once every twelve months during the term of the Agreement and during normal business hours unless otherwise decided by CrowdStrike in its sole discretion, CrowdStrike shall make appropriate CrowdStrike personnel reasonably available to Customer to discuss CrowdStrike's manner of compliance with applicable security obligations under this Agreement. In advance of such discussion, CrowdStrike may, in addition to the Security Documentation, provide Customer with access to additional requested information or documentation concerning CrowdStrike's information security practices as they relate to this Agreement, including without limitation, access to any security assessment reports designed to be shared with third parties. Any information or documentation provided pursuant to this assessment process or otherwise pursuant to this Schedule shall be considered CrowdStrike's Confidential Information and subject to the Confidentiality section of the Agreement.

7. **Customer Obligations**. Customer, along with its Affiliates, represents and warrants that: (i) it owns or has a right of use from a third party, and controls, directly or indirectly, all of the software, hardware and computer systems (collectively, "Systems") where the Products and/or CrowdStrike Tools will be installed or that will be the subject of, or investigated during, the Offerings, (ii) to the extent required under any federal, state, or local U.S. or non-US laws (e.g., Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq., Title III, 18 U.S.C. 2510 et seq., and the Electronic Communications Privacy Act, 18 U.S.C. § 2701 et seq.) it has authorized CrowdStrike to access the Systems and process and transmit data through the Offerings and CrowdStrike Tools in accordance with this Agreement and as necessary to provide and perform the Offerings, (iii) it has a lawful basis in having CrowdStrike investigate the Systems, process the Customer Data and the Personal Data; (iv) that it is and will at all relevant times remain duly and effectively authorized to instruct CrowdStrike to carry out the Offerings, and (v) it has made all necessary disclosures, obtained all necessary consents and government authorizations required under applicable law to permit the processing and international transfer of Customer Data and Customer Personal Data from each Customer and Customer Affiliate, to CrowdStrike.

8. **Notices**. The following individuals shall be the primary contacts at Customer and CrowdStrike for any coordination, communications or notices with respect to Personal Data and this Schedule:

   a. **CrowdStrike:** Drew Bagley, VP & Counsel, Privacy & Cyber Policy (drew.bagley@crowdstrike.com with a copy to legal@crowdstrike.com). For any Security Breach: Jerry Dixon, Chief Information Security Officer (jerry.dixon@crowdstrike.com with a copy to security@crowdstrike.com).
   b. **Customer:** the person who has signed the Agreement or another person as otherwise designated in writing (including by email) by Customer to CrowdStrike. Each party shall promptly notify the other if any of the foregoing contact information changes.

Appendix 1
Information Security Controls for CrowdStrike Systems

Security Control Category	Description
1. Governance	a. Assign to an individual or a group of individuals appropriate roles for developing, coordinating, implementing, and managing CrowdStrike's administrative, physical, and technical safeguards designed to protect the security, confidentiality, and integrity of Personal Data b. Use of data security personnel that are sufficiently trained, qualified, and experienced to be able to fulfill their information security-related functions
2. Risk Assessment	a. Conduct periodic risk assessments designed to analyze existing information security risks, identify potential new risks, and evaluate the effectiveness of existing security controls b. Maintain risk assessment processes designed to evaluate likelihood of risk occurrence and material potential impacts if risks occur c. Document formal risk assessments d. Review formal risk assessments by appropriate managerial personnel
3. Information Security Policies	a. Create information security policies, approved by management, published and communicated to all employees and relevant external parties. b. Review policies at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
4. Human Resources Security	**a.** Maintain policies requiring reasonable background checks of any new employees who will have access to Personal Data or relevant CrowdStrike Systems, subject to local law b. Regularly and periodically train personnel on information security controls and policies that are relevant to their business responsibilities and based on their roles within the organization
5. Asset Management	a. Maintain policies establishing data classification based on data criticality and sensitivity b. Maintain policies establishing data retention and secure destruction requirements c. Implement procedures to clearly identify assets and assign ownership
6. Access Controls	a. Identify personnel or classes of personnel whose business functions and responsibilities require access to Personal Data, relevant CrowdStrike Systems and the organization's premises b. Maintain controls designed to limit access to Personal Data, relevant CrowdStrike Systems and the facilities hosting the CrowdStrike Systems to authorized personnel c. Review personnel access rights on a regular and periodic basis d. Maintain physical access controls to facilities containing CrowdStrike Systems, including by using access cards or fobs issued to CrowdStrike personnel as appropriate e. Maintain policies requiring termination of physical and electronic access to Personal Data and CrowdStrike Systems after termination of an employee f. Implement access controls designed to authenticate users and limit access to CrowdStrike Systems g. Implement policies restricting access to the data center facilities hosting CrowdStrike Systems to approved data center personnel and limited and approved CrowdStrike personnel h. Maintain dual layer access authentication processes for CrowdStrike employees with administrative access rights to CrowdStrike Systems
7. Cryptography	a. Implement encryption key management procedures b. Encrypt sensitive data using a minimum of AES/128 bit ciphers in transit and at rest
8. Physical Security	a. Require two factor controls to access office premises b. Register and escort visitors on premises
9. Operations Security	a. Perform periodic network and application vulnerability testing using dedicated qualified internal resources b. Contract with qualified independent 3rd parties to perform periodic network and application penetration testing c. Implement procedures to document and remediate vulnerabilities discovered during vulnerability and penetration tests

10. Communications Security	a. Maintain a secure boundary using firewalls and network traffic filtering b. Require internal segmentation to isolate critical systems from general purpose networks c. Require periodic reviews and testing of network controls
11. System Acquisition, Development and Maintenance	a. Assign responsibility for system security, system changes and maintenance b. Test, evaluate and authorize major system components prior to implementation
12. Supplier Relationships	Periodically review available security assessment reports of vendors hosting the CrowdStrike Systems to assess their security controls and analyze any exceptions set forth in such reports
13. Information Security Breach Management	a. Monitor the access, availability, capacity and performance of the CrowdStrike Systems, and related system logs and network traffic using various monitoring software and services b. Maintain incident response procedures for identifying, reporting, and acting on Security Breaches c. Perform incident response table-top exercises with executives and representatives from across various business units d. Implement plan to address gaps discovered during exercises e. Establish a cross-disciplinary Security Breach response team
14. Business Continuity Management	a. Design business continuity with goal of 99.9% uptime SLA b. Conduct scenario based testing annually
15. Compliance	a. Establish procedures designed to ensure all applicable statutory, regulatory and contractual requirements are adhered to

27. Exhibit B

Dispute Resolution Outside North America

If Customer's principal office is located outside North America as indicated in the Agreement, the terms and conditions of this Exhibit shall apply to all disputes arising out of or relating to this Agreement (excluding disputes regarding the actual or alleged violation of CrowdStrike's intellectual property rights or the collection of overdue invoices, which shall be governed by California law).

28. 1. For ALL principal offices outside North America:

a. Choice of Law. This Agreement, and the rights and duties of the parties arising from this Agreement, shall be governed by, construed, and enforced with the laws of the State of New York, excluding its conflicts-of-law principles. The Uniform Computer Information Transactions Act and the United Nations Convention on the International Sale of Goods shall not apply.

b. Arbitration. Any dispute, claim, or controversy arising out of or relating to this Agreement or the existence, breach, termination, enforcement, interpretation, or validity of the Agreement, including the determination of the scope or applicability of this Agreement to arbitrate, (each, a "**Dispute**") shall be referred to and finally resolved by arbitration under the rules and at the location identified below. The arbitral panel shall consist of three (3) arbitrators, selected as follows: each party shall appoint one (1) arbitrator; and those two (2) arbitrators shall discuss and select third arbitrator. If the two party-appointed arbitrators are unable to agree on a third arbitrator, the third arbitrator shall be selected in accordance with the applicable rules of the arbitration body. Each arbitrator shall be independent of each of the parties and shall have suitable experience and knowledge in the subject matter of the Dispute. The arbitrators shall have the authority to grant specific performance and to allocate between the parties the costs of arbitration (including service fees, arbitrator fees and all other fees related to the arbitration) in such equitable manner as the arbitrators may determine. Judgment upon the award so rendered may be entered in a court having jurisdiction or application may be made to such court for judicial acceptance of any award and an order of enforcement, as the case may be. Notwithstanding the foregoing, either party shall have the right to institute an action in a court of proper jurisdiction for preliminary injunctive relief pending a final decision by the arbitrator, provided that a permanent injunction and damages shall only be awarded by the arbitrator. The language to be used in the arbitral proceedings shall be English.

29. 2. For ONLY principal offices within Europe, the Middle East or Africa:

Any Dispute shall be referred to and finally resolved by arbitration under the London Court of International Arbitration Rules (which Rules are deemed to be incorporated by reference into this clause) on the basis that the governing law is as follows: (a) if Customer brings an action against CrowdStrike, then the governing law is the State of New York, USA, (b) if CrowdStrike brings an action against Customer, then the governing law is the laws of England and Wales. The seat, or legal place, of arbitration shall be London, England.

30. 3. For ONLY principal offices within Asia Pacific (including India), Australia & New Zealand:

Any Dispute shall be referred to and finally resolved by arbitration under the Rules of Conciliation and Arbitration of the International Chamber of Commerce in force on the date when the notice of arbitration is submitted in accordance with such Rules (which Rules are deemed to be incorporated by reference into this clause) on the basis that the governing law is as follows: (a) if Customer brings an action against CrowdStrike, then the governing law is the State of New York, USA, (b) if CrowdStrike brings an action against Customer, then the governing law is as follows: (i) for Customers in: (x) Asia Pacific (including India): the laws of England and Wales, (y) Australia and New Zealand: the laws of the State of New South Wales, Australia. In all cases, the seat, or legal place, of arbitration shall be Singapore.

31. 4. For ONLY principal offices within the Americas, excluding North America:

Any Dispute shall be referred to and finally resolved by arbitration under International Dispute Resolution Procedures of the American Arbitration Association in force on the date when the notice of arbitration is submitted in accordance with such Procedures (which Procedures are deemed to be incorporated by reference into this clause) on the basis that the governing law is the law of the State of New York, USA. The seat, or legal place, of arbitration shall be New York, New York, USA.

Exhibit C
Additional or Different Terms That May Apply to Certain Customers

A. For Australian Consumers Only.

A.1. For Customers that are consumers under the Australian Consumer Law, the following provisions apply**.**

The benefits of the warranty in Section 8 *Warranties & Disclaimer* of this Agreement are in addition to any other rights and remedies in relation to the Offerings that Customer may be entitled to under Australian Consumer Law. Our goods and services come with guarantees that cannot be excluded under the Australian Consumer Law. For major failures with the service, you are entitled: (i) to cancel your service contract with us; and (ii) to a refund for the unused portion, or to compensation for its reduced value. You are also entitled to choose a refund or replacement for major failures with goods. If a failure with the goods or a service does not amount to a major failure, you are entitled to have the failure rectified in a reasonable time. If this is not done you are entitled to a refund for the goods and to cancel the contract for the service and obtain a refund of any unused portion. You are also entitled to be compensated for any other reasonably foreseeable loss or damage from a failure in the goods or service.

The warranties in this Agreement are provided by CrowdStrike, Inc. at 150 Mathilda Place, Third Floor, Sunnyvale California, USA. To file a claim under this limited warranty, Customers must contact CrowdStrike at support@crowdstrike.com. CrowdStrike shall be responsible for any costs Customer incurs in making a warranty claim under this Agreement.

A.2. For Customers that are consumers under the Australian Consumer Law, Section 12 *Limited Liability* shall be replaced in its entirety with the following:

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT FOR LIABILITY FOR ANY AMOUNTS PAID OR PAYABLE TO THIRD PARTIES UNDER SECTION 9 (*INDEMNIFICATION*), CUSTOMER'S PAYMENT OBLIGATIONS, AND/OR ANY INFRINGEMENT OR MISAPPROPRIATION BY ONE PARTY OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY IN CONNECTION WITH THIS AGREEMENT OR THE SUBJECT MATTER HEREOF (UNDER ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STATUTE, TORT (INCLUDING NEGLIGENCE), INDEMNITIES (OTHER THAN EXPRESSLY STATED IN SECTION 9 (*INDEMNIFICATION*)), OR OTHERWISE) FOR ANY LOST PROFITS, REVENUE, OR SAVINGS, LOST BUSINESS OPPORTUNITIES, LOST DATA, OR SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES OR SUCH DAMAGES OR LOSSES WERE REASONABLY FORESEEABLE; OR (B) AN AMOUNT THAT EXCEEDS THE TOTAL FEES PAID OR PAYABLE TO CROWDSTRIKE FOR THE RELEVANT OFFERING DURING THAT OFFERING'S SUBSCRIPTION/ORDER TERM. THESE LIMITATIONS WILL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY REMEDY SPECIFIED IN THIS AGREEMENT. MULTIPLE CLAIMS SHALL NOT EXPAND THE LIMITATIONS SPECIFIED IN THIS SECTION A2.

SECTION A.2 DOES NOT SEEK TO LIMIT OR EXCLUDE THE LIABILITY OF CROWDSTRIKE OR ITS AFFILIATES IN THE EVENT OF DEATH OR PERSONAL INJURY CAUSED BY ITS NEGLIGENCE OR FOR FRAUD OR FOR ANY OTHER LIABILITY FOR WHICH IT IS NOT PERMITTED BY LAW TO EXCLUDE. TO THE EXTENT APPLICABLE, **THIS PROVISION MUST BE READ SUBJECT TO THE AUSTRALIAN CONSUMER LAW.**

B. For Customers Outside the United States and Australia. Some countries, states and provinces, including member states of the European Economic Area, do not allow certain exclusions or limitations of liability, therefore, the exclusions or limitation of liabilities and disclaimers of warranties in the Agreement may not fully apply to Customer if the laws directly applicable to CrowdStrike in the performance of this Agreement do not allow such terms.