Crown Commercial Service

G-Cloud 12 Call-Off Contract

This Call-Off Contract for the G-Cloud 12 Framework Agreement (RM1557.12) includes:

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.

Digital Marketplace service ID number	591023384887782
Call-Off Contract reference	Buyer reference: Project_5036
Call-Off Contract title	KnowBe4 Security Awareness Training & Phishing Simulation
Call-Off Contract description	Strengthen the foundations of positive cyber security by undertaking regular planned awareness activities.
Start date	25/01/2021
Expiry date	24/01/2023 Option to extend for 12 months until 24/01/2024
Call-Off Contract value	[redacted] [redacted] [redacted] Total three year cost - £139,608.67 All figures are exclusive of VAT.
Charging method	Electronic payment.
Purchase order number	Purchase order will be provided following contract signature.

This Order Form is issued under the G-Cloud 12 Framework Agreement (RM1557.12).

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 Deliverables 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	The Secretary of State for Education Sanctuary Buildings 20 Great Smith Street Westminster London SW1P 3BT
To the Supplier	Actisoft Technology Limited 0203 931 0199 71-75 Shelton Street Covent Garden London WC2H 9JQ Company number: 10947250
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: Security Awareness Lead

Name: [redacted]
Email: [redacted]

Phone: [redacted]

For the Supplier:

Title: Managing Director

Name: [redacted]

Email: [redacted]

Phone: [redacted]

Call-Off Contract term

Start date	This Call-Off Contract Starts on **25/01/2021** and is valid for **24 Months.** The date and number of days or months is subject to clause 1.2 in Part B below.
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	This Call-off Contract can be extended by the Buyer for 1 period of 12 months, by giving the Supplier at least 30 days written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8. The extension period after 24 months should not exceed the maximum permitted under the Framework Agreement which is 2 periods of up to 12 months each. If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance: https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service

Buyer contractual details

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

G-Cloud lot	This Call-Off Contract is for the provision of Services under: • Lot 2: Cloud software
G-Cloud services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below: [redacted] If there is a service that won't begin on the Start date, then simply put 'zero'.

Location	The Services will be delivered to **DfE Cyber& Information Security Division**
Quality standards	The quality standards required for this Call-Off Contract are **Provision of access to KnowB4 Security software and functionality as described by KnowB4 Diamond subscription on the date of contract signing.**
Technical standards:	The technical standards used as a requirement for this Call-Off Contract are • **Unlimited Training and Phishing Simulation Use** • **Social Engineering Indicators** • **Integration with Active Directory** • **Advanced Reporting with 60+ Reports** • **Upload Your Own Content** • **Customisable Phishing Templates and Landing Pages** • **Phish Alert Button to forward emails to your Security Team** • **Engaging Interactive Browser-Based Training Content** • **Virtual Risk Officer**
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are **99.9% Service Availability** This may include any specific service levels or availability criteria required in the delivery of the services. You can only use the service levels or availability criteria: • in the Supplier's Service Definition • in the Service Description used as a requirement or acceptance criteria.

Onboarding	The onboarding plan for this Call-Off Contract is: **This is software by subscription – Onboarding tasks will be listed from completion of a KnowB4 Questionnaire. Account activation will take place and account credentials provided to DfE Project Manager [redacted].** The onboarding tasks will include: • Provision of credential and access to the service • Assistance in setting up user admin accounts. • Assistance in uploading staff data, sorting and making ready for use by all the service features. • Walkthrough of the security platform and its features • Walkthrough of the Phish-ER service and the features. • Instructions provided on the set up of the platform to a degree which enables staff in DfE to use the Phishing Simulation Capability, Learning Modules, Phish Alert Button, and Virtual Risk Agent.
Offboarding	The offboarding plan for this Call-Off Contract is • **The offboarding plan for this Call-Off Contract is to be planned with the buyer at least 6 months prior to contract ending and at no extra cost to the buyer.**
Collaboration agreement	Not applicable.

Limit on Parties' liability	The annual total liability for Buyer Data Defaults will not exceed [redacted] of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). [Clause 24.1 in Part B below applies for a more in-depth definition of Buyer Data Defaults, while still maintaining the definitions and meanings of Buyer Data and Default in Schedule 6: Glossary and Interpretations below.] The annual total liability for all other Defaults will not exceed [redacted] of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). [Clause 24.1 in Part B below provides a definition of Other Defaults.]
Insurance	The 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 [redacted] for each individual claim or any higher limit the Buyer requires (and as required by Law) ● employers' liability insurance with a minimum limit of [redacted] or any higher minimum limit required by Law

Force majeure	Neither party to this Agreement will be liable for delays or failures in performance under this Agreement (other than the payment obligations or breach of confidentiality requirements) resulting from acts or events beyond the reasonable control of such party, including acts of war, terrorism, acts of God, natural disasters (fires, explosions, earthquakes, hurricane, flooding, storms, explosions, infestations), embargos, riots, sabotage, governmental acts, provided that the delayed party: (a) gives the other party notice of such cause without undue delay; and (b) uses its reasonable commercial efforts to promptly correct such failure or delay in performance. A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 20 consecutive working days.
Audit	The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits (7.4 to 7.12)
Buyer's responsibilities	The Buyer is responsible for ensuring the software and service is used with KnowB4s terms and conditions of service.
Buyer's equipment	The Buyer's equipment to be used with this Call-Off Contract includes **None** Reason **No equipment is provided as part of this contract**

Supplier's information

Subcontractors or partners	The following is a list of the Supplier's Subcontractors or Partners' **Software supplier – KnowB4**

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 electronic payment.
Payment profile	[redacted]
Invoice details	The Supplier will issue electronic invoices annually in advance. The Buyer will pay the Supplier within [redacted] days of receipt of a valid invoice.
Who and where to send invoices to	Invoices will be sent to [redacted]
Invoice information required	All invoices must include Project Reference: Project_5036 - IT611
Invoice frequency	Invoice will be sent to the Buyer - Annually
Call-Off Contract value	The total value of this Call-Off Contract is £139,608.67

Call-Off Contract charges	[redacted] Total three year cost - £139,608.67 All figures are exclusive of VAT.

Additional Buyer terms

Performance of the Service and Deliverables	This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones: As this is software by subscription – implementation plans will be the responsibility of buyer alone. Support will be provided in onboarding, technical support and offboarding as described in this contract.
Personal Data and Data Subjects	Annex 1 (and Annex 2, if applicable) of Schedule 7 is being used.

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 RM1557.12.

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

Signed	Supplier	Buyer
Name		
Title		
Signature		
Date		

Schedule 1: Services

Unlimited Phishing Security Tests

Automated Security Awareness Program (ASAP)

Security ‘Hints & Tips’

Training Access Level I

Automated Training Campaigns

Brandable Content

Assessments

Phish Alert Button

Phishing Reply Tracking

Active Directory Integration (ADI)

Industry Benchmarking

Virtual Risk Officer™

Advanced Reporting

Crypto-Ransom Guarantee

Training Access Level II

Monthly Email Exposure Check

Vishing Security Test

Smart Groups

Reporting APIs

User Event API

Security Roles

Social Engineering Indicators (SEI)

USB Drive Test

Priority Level Support

Training Access Level III

AIDA™ Artificial Intelligence-driven Agent BETA

PhishER™ -

Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Digital Marketplace 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:

[redacted]

Customer Benefits

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

G-Cloud 12 Customer Benefits 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 24 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 2 periods of up to 12 months each.

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 extend the contract beyond 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:

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.6 (Relationship)
- 8.9 to 8.11 (Entire agreement)
- 8.12 (Law and jurisdiction)
- 8.13 to 8.14 (Legislative change)
- 8.15 to 8.19 (Bribery and corruption)
- 8.20 to 8.29 (Freedom of Information Act)
- 8.30 to 8.31 (Promoting tax compliance)
- 8.32 to 8.33 (Official Secrets Act)
- 8.34 to 8.37 (Transfer and subcontracting)
- 8.40 to 8.43 (Complaints handling and resolution)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.51 to 8.53 (Publicity and branding)
- 8.54 to 8.56 (Equality and diversity)
- 8.59 to 8.60 (Data protection

- 8.64 to 8.65 (Severability)
- 8.66 to 8.69 (Managing disputes and Mediation)
- 8.80 to 8.88 (Confidentiality)
- 8.89 to 8.90 (Waiver and cumulative remedies)
- 8.91 to 8.101 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretation
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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' 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 4 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

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

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

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

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

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

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

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

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

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

5. Due diligence

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

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

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

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

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

6. Business continuity and disaster recovery

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

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

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

7. Payment, VAT and Call-Off Contract charges

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

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

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

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

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

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

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

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

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

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

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

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

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 Subject to clause 24.1 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 the Data Protection Legislation or under incorporated Framework Agreement clauses 8.80 to 8.88. 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 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its Licensors.

11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.

11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.

11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.

11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown 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:

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

11.5.2 Supplier's performance of the Services

11.5.3 use by the Buyer of the Services

11.6 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:

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

11.6.2 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

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

11.7 Clause 11.5 will not apply if the IPR Claim is from:

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

11.7.3 other material provided by the Buyer necessary for the Services

11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

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

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

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

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

13. Buyer data

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

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

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

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

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

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

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

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: https://www.cpni.gov.uk/content/adopt-risk-management-approach 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/technology-code-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 (and the Buyer of any Buyer Confidential Information breach). 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 is reasonable compensation and covers 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); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability)

- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.89 to 8.90 (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 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 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 extend the Term beyond 24 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 extension 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 the number of consecutive days set out in the Order Form, 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 4.2 to 4.7, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:

24.1.1 Property: for all Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form

24.1.2 Buyer Data: for all Defaults by the Supplier resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data, will not exceed the amount in the Order Form

24.1.3 Other Defaults: for all other Defaults by either party, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form.

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

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

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

29.5 The Supplier will 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.

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

29.6.1 its failure to comply with the provisions of this clause

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

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

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

30. Additional G-Cloud services

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

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

31. Collaboration

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

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

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

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

32. Variation process

32.1 The Buyer can request in writing a change to this Call-Off Contract 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, clauses 8.59 and 8.60 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.59 and 8.60 are reproduced in this Call-Off Contract document at schedule 7.

Schedule 3: Collaboration agreement

Not applicable.

Schedule 4: Alternative clauses

1. Introduction

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

2. Clauses selected

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

2.1.1 Scots Law and Jurisdiction

2.1.2 References to England and Wales in incorporated Framework Agreement clause 8.12 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.

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

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

2.1.5 Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.2.

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

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

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

2.3 Discrimination

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

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

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

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

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

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

2.4 Equality policies and practices

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

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

a. the issue of written instructions to staff and other relevant persons

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

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

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

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

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

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

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

2.5 Equality

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

2.5.2 The Supplier acknowledges that the Customer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours

to assist (and to ensure that relevant Subcontractor helps) the Customer in relation to same.

2.6 Health and safety

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

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

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

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

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

2.7 Criminal damage

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

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

2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Customer will also make and pursue a claim diligently under the Compensation

Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Customer's cost and the Supplier will (at no additional cost to the Customer) provide any help the Customer reasonably requires with the appeal.

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

Schedule 5: Guarantee

Not applicable.

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) 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 Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
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 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 Framework Agreement 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)	Data Protection Legislation means: (i) the GDPR, the LED and any applicable national implementing Laws 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 including if applicable legally binding guidance and codes of practice issued by the Information Commissioner
Data Subject	Takes the meaning given in the 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.
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.

Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-for-tax
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 RM1557.12 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 Section 2 (Services Offered) 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.
GDPR	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
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 CCS'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, enforceable right within the meaning of Section 2 of the European Communities Act 1972, 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.
LED	Law Enforcement Directive (EU) 2016/680.
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 section 6 (What you report to CCS).
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 GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR.
Processor	Takes the meaning given in the GDPR.

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

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

Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-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: GDPR Information

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

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: [**Insert Contact details**]
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.

Descriptions	**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 paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller, and the Supplier is the Processor of the following Personal Data: ● All DfE staff data on the KnowBe4 security awareness platform. ● All metrics relating to DfE staff on the KnowBe4 security awareness platform.
Duration of the Processing	25/01/2021 to 24/01/2024
Nature and purposes of the Processing	Supplier will provide KnowBe4 software to DfE and this will be used to process DfE data. The data will include: • Work email address • Last name • First name • Team/business area • Office Location DfE will process this data on the supplier platform to:

	• Deliver learning to staff. • Deliver simulated phishing emails to staff. • Deliver security communications to staff. • Measure staff engagement with communications, phishing campaigns and learning materials. This is measure from an individual level, directorate, custom grouping, department. • Measure staff performance with learning quizzes, phishing simulations. This is measure from an individual level, directorate, custom grouping, department. • Provide audit of staff completing security activities. • Provide risk analysis of suspicious emails reported by staff, recording staff member, and responding to staff reports. • Providing instant feedback to staff on when they have identified a phishing simulation. This will happen over the space of 24 months with an update to the user list every month to confirm staff that have joined and left the department. The data held by the supplier will be stored/processed/destroyed in line with departmental requirements. A contract will be in place with the supplier which includes mandatory information security contract clauses. Security assurance of the supplier has been carried out by the Information security team and the supplier's security processes confirmed to be in line with DfE requirements.
Type of Personal Data	• Work email address • Last name • First name • Team/business area • Office Location • Age • Grade • Time served in the department • Temporary / perm/ contractor / work placement
Categories of Data Subject	Staff Data
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	At the end of the contract all user information on the Security Awareness Platform is hard wiped, and the server used is formatted and never re-used. Any DfE personal data supplied by Buyer / or held by supplier, will be securely deleted withing 30 days of the contract ending.

Annex 2: Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2 to 15 of Schedule 4 of the Framework Agreement (Where one Party is Controller and the other Party is Processor) and paragraphs 17-27 of Schedule 4 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the :

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

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

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

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

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

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

2. Undertakings of both Parties

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

(a) report to the other Party every **three** months on:

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

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

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

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

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

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

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses

2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

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

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

(g) take all reasonable steps to ensure the reliability and integrity of any of its personnel who have access to the Personal Data and ensure that its personnel:

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

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

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

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

(i) nature of the data to be protected;
(ii) harm that might result from a Data Loss Event;
(iii) state of technological development; and
(iv) cost of implementing any measures;

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

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

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

3. Data Protection Breach

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

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

(b) all reasonable assistance, including:

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

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

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

and/or

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

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

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

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

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

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

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

4. Audit

4.1 The Supplier shall permit:

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

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

under the control of any third party appointed by the Supplier to assist in the provision of the Services.

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

5. Impact Assessments

5.1 The Parties shall:

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

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

6. ICO Guidance

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

7. Liabilities for Data Protection Breach

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

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

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

(b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these

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

(c) if no view as to responsibility is expressed by the Information Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any Financial Penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the procedure set out in clauses 8.66 to 8.79 of the Framework terms (Managing disputes).

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

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

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

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

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

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

8. Not used

9. Termination

9.1 If the Supplier is in material Default under any of its obligations under this Annex 2 (joint controller agreement), the Buyer shall be entitled to terminate the contract by issuing a termination notice to the Supplier in accordance with Clause 18.5 (Ending the contract).

10. Sub-Processing

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

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

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

11. Data Retention

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

12. Departmental Security Standards for Business Services and ICT Contracts

"BPSS" "Baseline Personnel Security Standard"	means the Government's HMG Baseline Personal Security Standard . Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard
"CCSC" "Certified Cyber Security Consultancy"	is the National Cyber Security Centre's (NCSC) approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. See website: https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy
"CCP" "Certified Professional"	is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession. See website: https://www.ncsc.gov.uk/information/about-certified-professional-scheme
"CPA" "Commercial Product Assurance" [formerly called "CESG Product Assurance"]	is an 'information assurance scheme' which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards.. See website: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa

“Cyber Essentials” “Cyber Essentials Plus”	Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme. There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to these providers: https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body
“Data” “Data Controller” “Data Protection Officer” “Data Processor” “Personal Data” “Personal Data requiring Sensitive Processing” “Data Subject”, “Process” and “Processing”	shall have the meanings given to those terms by the Data Protection Act 2018
"Department’s Data" “Department’s Information”	is any data or information owned or retained in order to meet departmental business objectives and tasks, including: (a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Contractor by or on behalf of the Department; or (ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or (b) any Personal Data for which the Department is the Data Controller;
“DfE” “Department”	means the Department for Education
“Departmental Security Standards”	means the Department’s security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver.
“Digital Marketplace / G-Cloud”	means the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects.

End User Devices	means the personal computer or consumer devices that store or process information.
“Good Industry Practice” “Industry Good Practice”	means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
“Good Industry Standard” “Industry Good Standard”	means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
“GSC” “GSCP”	means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications
“HMG”	means Her Majesty’s Government
“ICT”	means Information and Communications Technology (ICT) and is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution
“ISO/IEC 27001” “ISO 27001”	is the International Standard for Information Security Management Systems Requirements
“ISO/IEC 27002” “ISO 27002”	is the International Standard describing the Code of Practice for Information Security Controls.
“ISO 22301”	is the International Standard describing for Business Continuity
“IT Security Health Check (ITSHC)” “IT Health Check (ITHC)” “Penetration Testing”	means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.
“Need-to-Know”	means the Need-to-Know principle employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties.
“NCSC”	The National Cyber Security Centre (NCSC) is the UK government’s National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk

"OFFICIAL" "OFFICIAL-SENSITIVE"	the term 'OFFICIAL' is used to describe the baseline level of 'security classification' described within the Government Security Classification Policy (GSCP). the term 'OFFICIAL–SENSITIVE is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the GSCP.
"RBAC" "Role Based Access Control"	means Role Based Access Control. A method of restricting a person's or process' access to information depending on the role or functions assigned to them.
"Storage Area Network" "SAN"	means an information storage system typically presenting block based storage (i.e. disks or virtual disks) over a network interface rather than using physically connected storage.
"Secure Sanitisation"	means the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. NCSC Guidance can be found at: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction
"Security and Information Risk Advisor" "CCP SIRA" "SIRA"	means the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also: https://www.ncsc.gov.uk/articles/about-certified-professional-scheme
"Senior Information Risk Owner" "SIRO"	means the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for overseeing the management of information risk across the organisation. This includes its executive agencies, arms length bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties.
"SPF" "HMG Security Policy Framework"	means the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government's Official Committee on Security

	on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. https://www.gov.uk/government/publications/security-policy-framework

12.1. The Contractor shall be aware of and comply the relevant HMG security policy framework, NCSC guidelines and where applicable DfE Departmental Security Standards for Contractors which include but are not constrained to the following clauses.

12.2. Where the Contractor will provide products or services or otherwise handle infor-mation at OFFICIAL for the Department, the requirements of Cabinet Office Pro-curement Policy Note – Use of Cyber Essentials Scheme certification - Action Note 09/14 dated 25 May 2016, or any subsequent updated document, are mandated; that "contractors supplying products or services to HMG shall have achieved, and will be expected to retain certification at the appropriate level for the duration of the contract. The certification scope shall be relevant to the services supplied to, or on behalf of, the Department.

12.3 Where clause 12.2 above has not been met, the Contractor shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements).

The ISO/IEC 27001 certification must have a scope relevant to the services supplied to, or on behalf of, the Department. The scope of certification and the statement of applicability must be acceptable, following review, to the Department, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

12.4 The Contractor shall follow the UK Government Security Classification Policy (GSCP) in respect of any Departmental Data being handled in the course of provid-ing this service and will handle all data in accordance with its security classification. (In the event where the Contractor has an existing Protective Marking Scheme then the Contractor may continue to use this but must map the HMG security classifica-tions against it to ensure the correct controls are applied to the Departmental Da-ta).

12.5 Departmental Data being handled in the course of providing an ICT solution or service must be separated from all other data on the Contractor's or sub-contractor's own IT equipment to protect the Departmental Data and enable the data to be identified and securely deleted when required in line with clause 12.14.

12.6 The Contractor shall have in place and maintain physical security to premises and sensitive areas in line with ISO/IEC 27002 including, but not limited to, en-try control mechanisms (e.g. door access), CCTV, alarm systems, etc.

12.7 The Contractor shall have in place and maintain an appropriate user access control policy for all ICT systems to ensure only authorised personnel have access to De-partmental Data. This policy should include appropriate segregation of duties and if applicable role based access controls (RBAC).

12.8 The Contractor shall have in place and shall maintain procedural, personnel, physi-cal and technical safeguards to protect Departmental Data, including but not limited to:

- physical security controls;
- good industry standard policies and processes;

- malware protection;
- boundary access controls including firewalls;
- maintenance and use of fully supported software packages in accordance with vendor recommendations;
- software updates and patching regimes including malware signatures, for op-erating systems, network devices, applications and services;
- user access controls, and;
- the creation and retention of audit logs of system, application and security events.

12.9 The contractor shall ensure that any departmental data (including email) transmit-ted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

12.10 The contractor shall ensure that any departmental data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certifi-cation process agreed with the department except where the department has given its prior written consent to an alternative arrangement.

12.11 The contractor shall ensure that any device which is used to process departmental data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security and https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles.

12.12 Whilst in the Contractor's care all removable media and hardcopy paper docu-ments containing Departmental Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer re-quired, using either a cross-cut shredder or a professional secure disposal organi-sation.

The term 'lock and key' is defined as: "securing information in a lockable desk drawer, cupboard or filing cabinet which is under the user's sole control and to which they hold the keys".

12.13 When necessary to hand carry removable media and/or hardcopy paper docu-ments containing Departmental Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthor-ised person has either visual or physical access to the material being carried. This clause shall apply equally regardless of whether the material is being carried inside or outside of company premises.

The term 'under cover' means that the information is carried within an opaque folder or envelope within official premises and buildings and within a closed briefcase or other similar bag or container when outside official premises or buildings.

12.14 In the event of termination of contract due to expiry, liquidation or non-performance, all information assets provided, created or resulting from the service shall not be considered as the supplier's assets and must be returned to the de-partment and written assurance obtained from an appropriate officer of the supply-ing organisation that these assets regardless of location and format have been fully sanitised throughout the organisation in line with clause 12.15.

12.15 In the event of termination, equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored by the Contractor must be accounted for and either physically re-turned or securely sanitised or destroyed in accordance with the current HMG poli-cy using an NCSC approved product or method.

Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as data stored in a cloud system, Storage Area Network (SAN) or on shared backup tapes, then the Contractor or sub-contractor shall protect the Department's information and data until such time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.

Evidence of secure destruction will be required in all cases.

12.16 Access by Contractor or sub-contractor staff to Departmental Data shall be con-fined to those individuals who have a "need-to-know" in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Se-curity Vetting clearance as required by the Department. All Contractor or sub-contractor staff must complete this process before access to Departmental Data is permitted.

12.17 All Contractor or sub-contractor employees who handle Departmental Data shall have annual awareness training in protecting information.

12.18 The Contractor shall, as a minimum, have in place robust Business Continuity ar-rangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the contract is not ad-versely affected in the event of an incident. An incident shall be defined as any sit-uation that might, or could lead to, a disruption, loss, emergency or crisis to the services delivered. If a ISO 22301 certificate is not available the supplier will pro-vide evidence of the effectiveness of their ISO 22301 conformant Business Conti-nuity arrangements and processes including IT disaster recovery plans and proce-dures. This should include evidence that the Contractor has tested or exercised these plans within the last 12 months and produced a written report of the out-come, including required actions.

12.19 Any suspected or actual breach of the confidentiality, integrity or availability of De-partmental Data handled in the course of providing this service shall be recorded as an incident. This includes any non-compliance with these Departmental Security Standards for Contractors, or other Security Standards pertaining to the solution.

Incidents shall be reported to the department immediately, wherever practical, even if unconfirmed or when full details are not known, but always within 24 hours of discovery. If incident reporting has been delayed by more than 24 hours, the contractor should provide an explanation about the delay.

Incidents shall be reported through the department's nominated system or service owner.

Incidents shall be investigated by the contractor with outcomes being notified to the Department.

12.20 The Contractor shall ensure that any IT systems and hosting environments that are used to handle, store or process Departmental Data shall be subject to independ-ent IT Health Checks (ITHC) using an NCSC CHECK Scheme ITHC provider be-fore go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Department and all necessary remedial work carried out. In the event of significant security issues be-ing identified, a follow up remediation test may be required.

12.21 The Contractor or sub-contractors providing the service will provide the Depart-ment with full details of any actual or future intent to develop, manage, support, process or store Departmental Data outside of the UK mainland. The Contractor or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Department.

12.22 The Department reserves the right to audit the Contractor or sub-contractors providing the service within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being

supplied and the Contractor's, and any sub-contractors', compliance with the clauses contained in this Section.

12.23 The Contractor and sub-contractors shall undergo appropriate security assurance activities and shall provide appropriate evidence including the production of the necessary security documentation as determined by the department. This will in-clude obtaining any necessary professional security resources required to support the Contractor's and sub-contractor's security assurance activities such as: a Secu-rity and Information Risk Advisor (SIRA) certified to NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Cyber Professional (CCP) schemes.

12.24 Where the Contractor is delivering an ICT solution to the Department they shall design and deliver solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current NCSC Information Assurance Guid-ance and Departmental Policy. The Contractor will provide the Department with ev-idence of compliance for the solutions and services to be delivered. The Depart-ment's expectation is that the Contractor shall provide written evidence of:

- Compliance with HMG Minimum Cyber Security Standard.
- Any existing security assurance for the services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification.
- Any existing HMG security accreditations or assurance that are still valid includ-ing: details of the awarding body; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement.
- Documented progress in achieving any security assurance or accreditation ac-tivities including whether documentation has been produced and submitted. The Contractor shall provide details of who the awarding body or organisation will be and date expected.

12.25 The Contractor shall contractually enforce all these Departmental Security Stand-ards for Contractors onto any third-party suppliers, sub-contractors or partners who could potentially access Departmental Data in the course of providing this service.

SCHEDULE 8: KnowBe4 Terms & Conditions

THESE TERMS OF SERVICE (THE "**AGREEMENT**") GOVERN CUSTOMER'S ACCESS AND USE OF KNOWBE4'S PRODUCTS AND SERVICES, UNLESS CUSTOMER HAS FULLY EXECUTED A MASTER AGREEMENT WITH KNOWBE4 IN WHICH CASE SUCH MASTER AGREEMENT GOVERNS, OR UNLESS CUSTOMER HAS FULLY EXECUTED AN END USER LICENSE AGREEMENT ("**EULA**") WITH AN AUTHORIZED KNOWBE4 CHANNEL PARTNER FOR THE PROVISION OF KNOWBE4 PRODUCTS AND SERVICES, IN WHICH CASE THAT EULA GOVERNS AND RELATED QUESTIONS ABOUT THE TERMS OF THE SUBSCRIPTION SHOULD BE DIRECTED TO THE AUTHORIZED KNOWBE4 CHANNEL PARTNER. CAPITALIZED TERMS HAVE THE DEFINITIONS SET FORTH HEREIN. BY ACCEPTING THIS AGREEMENT, EITHER BY: (1) CLICKING A BOX INDICATING ACCEPTANCE; (2) EXECUTING A QUOTE THAT REFERENCES THIS AGREEMENT; OR (3) USING KNOWBE4'S PRODUCTS AND SERVICES, CUSTOMER AGREES TO THE TERMS OF THIS AGREEMENT. IF THE INDIVIDUAL ACCEPTING THIS AGREEMENT IS ACCEPTING ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, SUCH INDIVIDUAL REPRESENTS THAT THEY HAVE THE AUTHORITY TO BIND SUCH ENTITY AND ITS AFFILIATES TO THESE TERMS AND CONDITIONS, IN WHICH CASE THE TERM "**CUSTOMER**" SHALL REFER TO SUCH ENTITY AND ITS AFFILIATES. IF THE INDIVIDUAL ACCEPTING THIS AGREEMENT DOES NOT HAVE SUCH AUTHORITY OR DOES NOT AGREE WITH THESE TERMS AND CONDITIONS, SUCH INDIVIDUAL MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT USE THE PRODUCTS SERVICES. Customer and KnowBe4 may be referred to in this Agreement individually as a "**party**" or jointly as the "**parties**." This Agreement governs all purchased Products and Services, as defined below, provided by KnowBe4 to Customer. KnowBe4 may update or make changes to these terms from time to time. KnowBe4 encourages Customer to periodically review and check this Agreement for updates to stay informed about the terms that govern Customer's use of the Products and Services. Customer's continued use of the Products and Services after KnowBe4 makes any changes is deemed to be an acceptance of those changes. The Products and Services may not be accessed for purposes of monitoring their availability, performance or functionality, or for any other benchmarking or competitive purposes, or as otherwise restricted by this Agreement. KnowBe4's direct competitors (or third party agents acting on behalf of such direct competitors) are prohibited from accessing the Products and Services.

1. **Definitions.** For purposes of this Agreement:

   "**Active User(s)**" means Customer's Users with active assigned Seats.

"**Affiliate**" means an entity that, directly or indirectly, through one or more entities, controls; is controlled by; or is under common control with, the specified entity.

"Beta Product" means the second phase of software testing in which a sampling of the intended audience samples a product prior to its general release and, in return, Customer provides KnowBe4 feedback about the Beta Product. Use of Beta Products by Customer is optional.

"**Confidential Information**" means all information or material disclosed by a party (the "**Disclosing Party**") to the other party (the "**Receiving Party**"), whether orally or in writing, which: (a) gives either party some competitive business advantage or opportunity of obtaining some competitive business advantage, or the disclosure of which may be detrimental to the interests of the Disclosing Party; and (b) is either (i) marked "Confidential," "Restricted," "Proprietary," or includes other similar markings, (ii) known by the parties to be confidential and proprietary, or (iii) from all the relevant circumstances should reasonably be assumed to be confidential and proprietary. The Products and Services are deemed Confidential Information of KnowBe4.

"Courseware" means training modules, games, posters, artwork, videos, newsletters, security documents, or other content and materials provided by KnowBe4.

"Direct Message Injection (DMI)" means a KnowBe4 product and add-on, specific to Microsoft 365 (formerly Office 365) that automatically bypasses Microsoft 365's protections to allow simulated phishing emails to reach the end user. Use of DMI by Customer is optional; in order to activate DMI, Customer must provide separate and specific permissions and authorizations in accordance with the Documentation. Customer has the ability to revoke any such access required to use DMI at any time. DMI is only applicable to Customers using Microsoft 365 for email.

"**Documentation**" means KnowBe4's then-current generally available documentation, specifications, user manuals, etc., for the Products and Services, located at https://knowbe4.zendesk.com/hc/en-us or such other URL locations on KnowBe4's website as KnowBe4 may provide from time to time.

"**KnowBe4**" means KnowBe4, Inc. and its Affiliates.

"**LMS**" means learning management system that is software for the administration, documentation, tracking, reporting, and delivery of Courseware, which includes any e-learning education courses or training programs. KnowBe4 provides a cloud-based LMS through its Web Hosted Services. Upon approval by KnowBe4, Customer may also opt to use its own, or a third party's, LMS in accordance with the terms of this Agreement.

"PhishER™" means a KnowBe4 product that enables Customer to identify and respond to any potential threats in its email system. PhishER includes features such as PhishML and PhishRIP.

"PhishML™" means a feature included with a subscription to PhishER that uses machine learning to enable Customer to prioritize its evaluation of all user-reported emails for potential threats. This feature may be deactivated at Customer's option at any time.

"PhishRIP™" means a feature included with a subscription to PhishER that enables the Customer to quarantine and permanently delete specific emails (i.e., emails identified as potential threats) from its email system. Use of PhishRIP by Customer is optional; in order to activate PhishRIP, Customer must provide separate and specific permissions and authorizations in accordance with the Documentation. Customer has the ability to revoke any such access required to use PhishRIP at any time.

"**Product Privacy Notice**" means KnowBe4's Product Privacy Notice, that may be found at https://www.knowbe4.com/product-privacy-notice, or such other URL locations on KnowBe4's website as KnowBe4 may provide from time to time.

"**Products**" means any Software, Services, Courseware, and/or Web Hosted Services that KnowBe4 offers to Customer, including any Documentation.

"**Product Support**" means any maintenance and support of any Products provided by KnowBe4.

"**Quote**" means a purchasing document or other similar document, such as a purchase order or statement of work ("**SOW**"), in connection with a purchase under this Agreement.

"**Seat(s)**" refers to the number of Users permitted access to the Products and/or Services pursuant to the user count purchased via a Quote.

"**Security Page**" means KnowBe4's security page that provides information about KnowBe4's information security practices which may be found at https://www.knowbe4.com/security, or such other URL locations on KnowBe4's website as KnowBe4 may provide from time to time.

"**Services**" means any professional services, including implementation and installation services, managed services, consultancy services, or services for the customization or branding of Courseware, agreed upon by the parties, and set forth in a Quote or any additional Product Support purchased pursuant to a Quote. KnowBe4 may require Customer to enter into a statement of work ("**SOW**") detailing the Services to be performed.

"**Software**" means the object code version of any software that may be licensed by Customer under this Agreement for installation on Customer's systems. To the extent KnowBe4 delivers any updates or enhancements to Customer as part of Product Support, such updates and enhancements will be deemed included in the definition of "Software."

"**User(s)**" means any of Customer's employees or its other third parties to whom Customer gives access to the Products and Services.

"**Web Hosted Services**" means an application and/or database product hosted by KnowBe4 or its agents and made available for remote access and use by Customer under this Agreement.

2. Products.

2.1 ***Software License.*** This Section applies only in the event Customer licenses Software from KnowBe4 or through an authorized KnowBe4 channel partner. Subject to Customer's commitment to payment in accordance with this Agreement, KnowBe4 hereby grants to Customer, for use with Customer's authorized Users, and solely for internal

business purposes and not for resale or publication, a limited; non-exclusive; non-sublicensable; non-transferable; royalty-free license to install, use, execute, display, and access the Software. The Term, as defined below, of the foregoing license will be as set forth in the applicable Quote. Apart from the foregoing limited licenses, Customer is not being granted any right, title, or interest in or to the Software, or otherwise the Products. All such rights are expressly reserved by KnowBe4. Some Software or components used in KnowBe4's Products may be offered under an open source license, which may be found at https://support.knowbe4.com/hc/en-us/articles/360000870387-Open-Source-Licensing-Information, or such other URL locations on KnowBe4's website as KnowBe4 may provide from time to time.

2.2 ***Courseware License.*** This Section applies only in the event Customer licenses Courseware from KnowBe4 or through an authorized KnowBe4 channel partner. Subject to Customer's commitment to payment in accordance with this Agreement, KnowBe4 hereby grants to Customer, for use with Customer's authorized Users, and solely for internal business purposes and not for resale or publication, a limited; non-exclusive; non-sublicensable; non-transferable; royalty-free license to install, use, execute, display, and access the Courseware. The Term, as defined below, of the foregoing license will be as set forth in the applicable Quote. Apart from the foregoing limited licenses, Customer is not being granted any right, title, or interest in or to the Courseware, or otherwise the Products. All such rights are expressly reserved by KnowBe4.

2.3 ***Web Hosted Services Access.*** This Section applies only in the event Customer orders Web Hosted Services from KnowBe4 or through an authorized KnowBe4 channel partner. Subject to Customer's commitment to payment in accordance with this Agreement, KnowBe4 hereby grants to Customer, for use with Customer's authorized Users, and solely for internal business purposes and not for resale or publication, a non-exclusive and non-transferable right to access and use the Web Hosted Services for its internal business purposes. The Term, as defined below, of the foregoing access right will be as set forth in the applicable Quote. Customer will be solely responsible for connection of Customer's systems to a telecommunications service that provides Internet access for purposes of Customer's access and use of the Web Hosted Services. KnowBe4 will use commercially reasonable efforts to make the Web Hosted Services available in accordance with the terms set forth in the SLA**.**

2.4 ***Beta Products*****.** KnowBe4 may offer Beta Products to Customer at no charge. Use of the Beta Products are at the election of Customer and are for evaluation purposes only. Beta Products are not considered "Services" and do not come with Product Support. Beta Products may be subject to additional terms. KnowBe4 reserves the right to discontinue the Beta Products at any time. Use of the Beta Products will automatically terminate at such time as KnowBe4 makes such Beta Products generally available. Beta

Products may be unpredictable and lead to erroneous results. Customer acknowledges and agrees that: (a) Beta Products are experimental and have not been fully tested; (b) Beta Products may not meet Customer's requirements; (c) the use or operation of any Beta Products may not be uninterrupted or error free; (d) Customer's use of any Beta Products is for purposes of evaluating and testing the Beta Products and for providing feedback to KnowBe4; (e) Customer will inform its employees, staff members, and other Users regarding the nature of Beta Products; and (f) Customer will hold all information relating to Beta Products and Customer's use of Beta Products, including any performance measurements and other data relating to Beta Products, in strict confidence and will not disclose such information to any unauthorized third parties. Customer will promptly report any errors, defects, or other deficiencies in any Beta Products to KnowBe4. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, ALL BETA PRODUCTS ARE PROVIDED "AS-IS" AND "AS-AVAILABLE," WITHOUT WARRANTIES OF ANY KIND. Customer hereby waives any and all claims, now known or later discovered, that Customer may have against KnowBe4 and KnowBe4's suppliers and licensors arising out of Customer's use of Beta Products.

2.5 ***Limited Access Account.*** In the event Customer is granted access or use of any Products on an evaluation or trial period basis, including any limited access accounts created by Customer, then, subject to the terms and conditions of this Agreement, KnowBe4 hereby grants Customer, solely for its internal business evaluation purposes: (a) a revocable, limited, non-exclusive, non-sublicensable, non-transferable license during the Limited Access Period to install, use, execute, display, and access the Software and/or Courseware included in the Products; and (b) a revocable, limited, non-exclusive, non-transferable, right to access and use the Web Services included in the Products made available to Customer by KnowBe4 for the Limited Access Period, subject to any terms or limitations expressly set forth in any activation email. Customer may only use such Products from the earlier of: (1) the date this Agreement is accepted by Customer; or (2) the date in which Customer was permitted access to the Products by way of an activation email, until the expiration date set forth in applicable activation email, or, if no expiration date is set forth in the applicable activation email, thirty (30) days after the earlier of either (a) or (b) herein (the "Limited Access Period"). Customer and KnowBe4 may extend the Limited Access Period upon mutual written agreement (including via email). This evaluation license and grant of access will terminate automatically upon expiration of the Limited Access Period. At any time prior to the end of the Limited Access Period, KnowBe4 may terminate the Limited Access Period for the Products without notice. Upon any termination, Customer shall discontinue use and/or access to the Products unless and until Customer has agreed to purchase a license or grant of access to use and/or access such Products. During the Limited Access Period, all terms and conditions of this Agreement will apply, except that (i) no fees will be due from Customer, unless otherwise specified; (ii) the Products will be provided without warranties

or indemnities of any kind and entirely on an "as-is" basis (e.g., Sections including Product Support, Product and Service Warranties and KnowBe4 Indemnity Obligations will not apply); and (iii) additional evaluation terms and conditions may appear on the trial registration web page or activation email sent by KnowBe4, on the applicable Quote provided by KnowBe4 or by way of a proof of concept agreement executed between the parties. Any such additional terms and conditions shall be incorporated into this Agreement by reference and are legally binding. Apart from the foregoing limited license and grant of access, Customer is not being granted any right, title, or interest in or to the Products. All such rights are expressly reserved by KnowBe4. CUSTOMER DATA ON KNOWBE4 SYSTEMS OR IN KNOWBE4'S POSSESSION OR CONTROL, REPORTS, AND ANY CUSTOMIZATIONS MADE TO THE PRODUCTS BY OR FOR CUSTOMER'S BENEFIT MAY BE PERMANENTLY LOST OR DELETED DURING THE LIMITED ACCESS PERIOD OR AT THE END OF THE LIMITED ACCESS PERIOD.

2.6 ***PhishER.*** This Section applies only in the event Customer orders PhishER from KnowBe4 or through an authorized KnowBe4 channel partner. For more information about PhishER and its additional features (such as PhishML and PhishRIP), Customer may refer to the Documentation. Customer is solely responsible for ensuring compliance with all applicable laws and regulations relating to Customer's use of PhishER. Customer acknowledges that PhishER may pose certain risks to Customer's email system. Customer is solely responsible for Customer's actions in the operation of PhishER and acknowledges KnowBe4 is not responsible for any of Customer's actions, nor is KnowBe4 responsible for backups to Customer's email system. CUSTOMER HEREBY WAIVES ANY COSTS, DAMAGES, OR EXPENSES ASSOCIATED WITH THESE RISKS AND HOLDS KNOWBE4 HARMLESS WITH RESPECT TO SUCH COSTS, DAMAGES, OR EXPENSES.

2.7 ***Direct Message Injection (DMI).*** This Section applies only in the event Customer: (a) utilizes Microsoft (formerly Office 365)365 for email; and (b) exercises the option to activate the DMI products and add-on from KnowBe4 or through an authorized KnowBe4 channel partner. For more information about DMI, Customer may refer to the Documentation. Customer is solely responsible for ensuring compliance with all applicable laws and regulations relating to its use of DMI. As a result, Customer acknowledges that DMI may pose certain risks to Customer's email system. Customer is solely responsible for the actions of its representatives in the operation of DMI and acknowledges KnowBe4 is not responsible for any actions of the Customer's representatives nor is it responsible for backups to the Customer's email system. CUSTOMER HEREBY WAIVES ANY COSTS, DAMAGES, OR EXPENSES ASSOCIATED WITH THESE RISKS AND HOLDS KNOWBE4 HARMLESS WITH RESPECT TO ANY SUCH COSTS, DAMAGES, OR EXPENSES.

3. Product Usage & Rights.

3.1 ***Acceptance.*** Customer is deemed to have committed to a purchase in full for the Products and Services (regardless of any split payment terms) once a Quote is sent to KnowBe4 for processing or once payment has been tendered through check, credit card, or other form of payment. Payment via check, credit card, or other form of tendering payment will be deemed acceptance of the corresponding Quote or invoice sent to Customer by KnowBe4. If Customer is an organization subject to certain fiscal period restrictions or appropriations, Customer hereby represents and warrants that Customer has the ability to pay all fees, regardless of any split payment terms, in full, out of Customer's current fiscal period's allocated budget or that Customer has the authority to legally commit to a purchase outside of the current fiscal period. Except as otherwise specified herein, all sales are final, non-refundable, and non-returnable except with respect to Products and Services that do not meet applicable specifications in the relevant Documentation or that are not identified in the Quote.

3.2 ***Operation of the Products.*** The implementation and operation of KnowBe4's Products, and any deliverables resulting from Services performed, are done so by designated admin(s) employed or contracted by Customer. Any Managed Services, as defined below, may be subject to additional fees.

3.3 ***Customer Users.*** The Products and Services are provided on a per-seat, subscription basis. The concurrent number of Active Users receiving access may not exceed the purchased number of Seats. If the number of Active Users exceed the purchased number of Seats, Customer is obligated to either pay for any Seats that surpass the purchased amount or immediately reduce its number of Active Users. Customer is not permitted to freely re-assign Seats to Users. KnowBe4 prohibits cycling of Seats amongst Customer's personnel. If an Active User's account is terminated or removed, that User's Seat license is no longer considered in use and may be allocated to another User upon written approval by KnowBe4. Notwithstanding the foregoing, KnowBe4's approval is not required in the instance an Active User's account is terminated or removed due to Customer's termination of that Active User's employment, or otherwise for termination of contract with that Active User, to account for Customer's normal attrition in workforce. Upon request by KnowBe4, Customer agrees to provide KnowBe4 with a certification of such compliance. KnowBe4 reserves the right to audit Customer's compliance with this Section. Additional Seats may be added mid-subscription term and such additional Seats will be co-pending with the then-current subscription term and will terminate on the same date. Add-ons for more Seats mid-term will be priced at the same volume/level discount purchased under the applicable co-pending Quote and will be valid only until the end of such co-pending subscription term. Upon renewal, new rates may apply.

3.4 ***Professional Services.*** In the instance Customer purchases Services to be performed by KnowBe4, Customer may be required to sign an SOW detailing the project specifications for the Services. Services may include, but are not limited to, the request for KnowBe4 to implement and operate the Products on behalf of Customer ("**Managed Services**"), additional maintenance and support (as opposed to any standard maintenance and support already included), customization and branding of any Courseware, and any additional consultancy or professional services. The completion time for any Services to be performed under an SOW, and any milestones, will be dependent on KnowBe4's receipt of all Customer assets and specifications necessary for the project, in addition to KnowBe4 receiving a validly signed SOW for processing, as requested by KnowBe4. The completion deadline will start from the date of delivery of all such assets and specifications, not the date of KnowBe4's receipt of the signed SOW. Customer acknowledges that delays in providing assets or specifications at the request of KnowBe4 for such Services may delay the completion of the Services. KnowBe4 will not be faulted for delays caused by Customer's failure to reasonably cooperate. Service hours purchased pursuant to an SOW or a Quote will expire upon the expiration or termination of Customer's subscription term and will not carry over to any subsequent renewal term.

3.5 ***Intellectual Property.*** This is not a work made-for-hire agreement, as defined by U.S. or other applicable law. KnowBe4 and its licensors own and reserve all right, title, and interest, including intellectual property rights, in the Products and all enhancements, modifications, and updates thereto. Except for express licenses granted in this Agreement, KnowBe4 is not granting or assigning to Customer any right, title, or interest, express or implied, in or to KnowBe4's intellectual property. KnowBe4 reserves all rights in such property.

3.6 ***Feedback.*** Customer may provide KnowBe4 with suggestions, comments, or other feedback (collectively, "**Feedback**") with respect to the Products. Feedback is voluntary. KnowBe4 is not obligated to hold any Feedback in confidence. KnowBe4 may use Feedback for any purpose without obligation of any kind. To the extent a license is required to make use of any intellectual property in any Feedback, Customer grants KnowBe4 an irrevocable, non-exclusive, perpetual, royalty-free license to use such Feedback in connection with KnowBe4's business, including the enhancement of the Products.

4. Data.

4.1 ***Customer Data.*** Customer grants KnowBe4 a non-exclusive, world-wide, royalty-free license to use the data and other information input by Customer into the Products ("**Customer Data**"): (a) to perform KnowBe4's obligations under this Agreement; (b) in compliance with the Product Privacy Notice; and (c) as may be required by law. Customer will be responsible for obtaining all rights, permissions, and authorizations to

provide the Customer Data to KnowBe4 for use as contemplated under this Agreement. Except for the limited license granted in this Section, nothing contained in this Agreement will be construed as granting KnowBe4 any right, title, or interest in the Customer Data. Customer Data will be deemed Customer Confidential Information.

4.2 ***Aggregated Data.*** KnowBe4 may also use Customer Data in an aggregate, de-identified, and generic manner for marketing; survey; and benchmarking purposes, in the review and development of current and future Products, Product usage, and other similar purposes ("**Aggregated Data**"). Aggregated Data: (a) is used only for internal administrative purposes and general usage statistics; (b) does not identify Customer or any individual; and (c) to the extent such Aggregated Data is disclosed, is only disclosed in a generic or aggregated manner for the purposes of sharing Product usage and statistical or benchmarking purposes. Aggregated Data will not be considered Customer Confidential Information.

4.3 ***Data Security.*** Customer Data is maintained in accordance with **the Information Security Requirements in this Agreement** using industry standard administrative, physical, and technical safeguards that are designed to provide for the protection of the security, confidentiality, and integrity of Customer Data. KnowBe4's security safeguards include means for preventing access, use, modification, and disclosure of Customer Data by unauthorized individuals. Notwithstanding the foregoing, Customer Data access may be provided: (a) to KnowBe4 and other personnel to the extent necessary to provide the Products, Services, and support; (b) as compelled by law; (c) as set forth in the Product Privacy Notice; or (d) as expressly permitted by Customer. KnowBe4's Products currently operate in third party datacenters located in the US or EU and have been built with high availability, business continuity, and disaster recovery in mind. KnowBe4's cloud architecture follows industry standard security practices and is regularly assessed for vulnerabilities and risks. Information about KnowBe4's information security practices may be found at KnowBe4's Security Page.

4.4 ***Data Protection.*** The collection, use, and disclosure of Customer Data in connection with Customer's use of the Products is subject to the Product Privacy Notice. By using the Products, Customer and each User acknowledge that the Customer Data will be processed in accordance with both the Product Privacy Notice and this Agreement and may be processed in a country where it was collected, as well as in countries where privacy laws may be different or less stringent, provided KnowBe4 ensures compliance with applicable data protection laws. By using the Products, or submitting Customer Data via the Products, Customer expressly consents to such processing. To the extent Customer or User provides personal data or other information belonging to a third party, Customer represents and warrants that it has that person's, organization's, or other such third party's proper consent, or otherwise proper authorization, to do so. In the event Customer enters into a Data Processing Agreement with KnowBe4, such

Data Processing Agreement will govern the data handling practices between the parties and will supersede the language contained in this Section in the event of a conflict.

4.4.1. ***Protected Health Information, Payment Card Information, and other Sensitive Information.*** KnowBe4 does not need, nor does KnowBe4 request, any protected health information ("**PHI**") governed by the Health Insurance Portability and Accountability Act and its implementing regulations ("**HIPAA**"). KnowBe4 does not need, nor does KnowBe4 request, any non-public consumer personally identifiable information or financial information governed by the Gramm-Leach-Bliley Act ("**GLBA**") or payment card information covered by the Payment Card Industry Data Security Standards ("**PCI DSS**") in order to provide KnowBe4's products and services. Customer should never disclose, nor allow to be disclosed, PHI, information protected by PCI DSS or GLBA, or other sensitive information to KnowBe4. Customer acknowledges that KnowBe4 does not take steps to ensure KnowBe4's products are GLBA, HIPAA, or PCI DSS compliant. All obligations of the aforementioned regulations remain solely with Customer. KnowBe4's Products and Services are not intended for use with minors (as defined by applicable law). Customer is prohibited from authorizing minors, as defined by applicable law, to use or access the Products and Services, except as otherwise provided in a signed writing by an authorized representative of KnowBe4.

5. Customer Obligations.

5.1 ***Connectivity.*** Customer is solely responsible for all telecommunication or Internet connections, and associated fees, required to access and use the Products, as well as all hardware and software. KnowBe4 is not responsible for: (a) Customer's access to the Internet; (b) interception or interruptions of communications through the Internet; or (c) changes or losses of data through the Internet.

5.2 ***User Credentials.*** Customer will ensure User credentials (e.g., usernames and passwords) remain confidential, and Customer and Users will not disclose any such credentials to any third party. In addition, Customer will notify KnowBe4 immediately upon discovery of an unauthorized disclosure of any such credentials or upon any unauthorized access. Upon any termination of the engagement or deactivation of any User with knowledge of any such credentials, Customer will immediately change such credentials and remove access for that User.

5.3 ***Use of Customer or Third Party LMS.*** In the event Customer uses its own or a third party's LMS, or other mechanisms for hosting Courseware or other such content provided by KnowBe4 or its third party licensors, Customer will ensure strict compliance in accordance with this Agreement and will ensure an agreement is in place with any such third party that contains substantially the same level of protection for the Courseware

and other such content as contained herein. After the termination of the applicable subscription term, Customer will ensure all Courseware and other such content is removed from such third party's possession.

5.4 ***Affiliates.*** Customer, if purchasing Seats on behalf of an Affiliate, will ensure its Affiliates comply with the terms of this Agreement. The use of the Products by the Affiliate and its Users represents acceptance of the terms of this Agreement by such Affiliate and its Users for which Customer will be jointly and severally liable with its Affiliate for any breach by the Affiliate of this Agreement. No Affiliate may directly enforce any provision of this Agreement. All actions to enforce this Agreement must be brought by Customer.

5.5 ***Restrictions*.**

5.5.1 Customer may not: (a) reverse engineer, disassemble, decompile, or otherwise attempt to reveal the trade secrets or know-how underlying the Products, except to the extent expressly permitted under applicable law; (b) use KnowBe4's intellectual property or Confidential Information to develop a product that is similar to the Products; (c) use any KnowBe4 Confidential Information to contest the validity of any KnowBe4 intellectual property; (d) remove or destroy any copyright notices, other proprietary markings, or confidentiality legends placed on or made available through the Products; or (e) use the Products in any manner or for any purpose inconsistent with the terms of this Agreement or the Documentation. Software will only be used by the licensed number of Active Users for whom Customer paid the applicable fees.

5.5.2 Access and use of KnowBe4 Products, Services, or other related materials (which the parties acknowledge are proprietary and Confidential Information of KnowBe4) is solely authorized for the internal business purposes of the Customer and Active Users, and only for the duration of the subscription term or evaluation period, as applicable. Use of KnowBe4 Products, Services, or other related materials for analytical or research purposes, to be used or disclosed outside of Customer's organization, is strictly prohibited. Sharing screenshots, downloads, or other forms of copying, duplicating, or replicating the Products, Services, or other related materials, publicly or outside of Active Users, is strictly prohibited. Customer acknowledges that some of KnowBe4's Products and Services are designed to assist Customer in training Users and may include developing, customizing, and sending fake cyber security attack campaigns for purposes of employee training, but that Customer, and not KnowBe4 or any KnowBe4 channel partners, will be responsible for Customer's compliance with all laws and governmental regulations, and any results in connection with the

Customer's use of the Products (including any reports or information produced in connection therewith).

5.5.3 Customer acknowledges and understands that if Customer is a direct competitor of KnowBe4 (or a third party acting on behalf of such direct competitor), Customer is not permitted to, and will not, access or use any KnowBe4 Products, Services, or other related materials, all of which are considered confidential and proprietary to KnowBe4.

6. Customer Content.

6.1 Depending on the Products and Services purchased via a Quote, Customer may use KnowBe4's Products and Services for the hosting of its assets, content, and other materials, such as certain reports; documents; manuals; audiovisual materials; photos; videos; and audio files, to make available to Active Users on or through the Products and Services ("**Customer Content**"). All Customer Content will be considered Customer Data. Subject to, and conditioned on, Customer's and Users' compliance with the terms and conditions of this Agreement, during the applicable subscription term, KnowBe4 will provide Customer and Active Users remote electronic access to the Customer Content through the Web Hosted Services in accordance with this Agreement. KnowBe4 has the right to: (a) take any action with respect to any Customer Content that it deems necessary or appropriate, in KnowBe4's sole discretion, including if KnowBe4 reasonably believes that such Customer Content violates this Agreement, infringes any intellectual property right or other right of any person or entity, threatens the personal safety of any person, or creates potential liability for KnowBe4; (b) take appropriate legal action including, without limitation, referral to law enforcement related to any illegal or unauthorized Customer Content provided by Customer; or (c) terminate or suspend Customer's access to the Web Hosted Services for any violation of this Agreement. Customer grants KnowBe4, its service providers, and each of their respective licensees, successors, and assigns the right to use, reproduce, modify, perform, display, distribute, and otherwise disclose the Customer Content as necessary to provide the Web Hosted Services and to make the Customer Content available to Customer and Users.

6.2 Customer represents and warrants that: (a) Customer owns all rights in and to the Customer Content and/or has the right to grant the licenses granted herein to KnowBe4, service providers, and each of their respective licensees, successors, and assigns; and (b) all Customer Content does and will continue to comply with this Agreement; (c) all Customer Content does and will continue to comply with all international, federal, state, and local laws and regulations; and (d) the Customer Content does not: (i) contain any material which is defamatory, obscene, indecent, abusive, offensive, violent, hateful, inflammatory, or otherwise objectionable; (ii) promote sexually explicit or

pornographic material, violence, or discrimination based on race, sex, religion, nationality, disability, sexual orientation, or age; (iii) infringe any patent, trademark, trade secret, copyright, or other intellectual property or other rights of any person; (iv) violate the legal rights (including the rights of publicity and privacy) of others or contain any material that may give rise to any civil or criminal liability under applicable laws or regulations or that otherwise may be in conflict with this Agreement; (v) promote any illegal activity, or advocate, promote, or assist any unlawful act; (vi) intentionally create unreasonable disturbances to any other person or organization; or (vii) contain any: (A) viruses, trojan horses, worms, backdoors, or other software or hardware devices, the effect of which would permit unauthorized access to, or disable, erase, or otherwise harm, any computer, systems, software, or content; or (B) time bombs, drop dead devices, or other software or hardware devices designed to disable a computer program automatically with the passage of time or under the positive control of any person, or otherwise deprive KnowBe4, or its customers/users, of its lawful rights.

6.3 In addition to Customer's indemnification obligations contained in this Agreement, Customer will defend and indemnify KnowBe4 and hold it harmless from any and all claims, losses, deficiencies, damages, liabilities, costs, and expenses (including, but not limited to, reasonable attorneys' fees) incurred by KnowBe4 as a result of any claim by a third party arising from KnowBe4's hosting or distribution of the Customer Content as authorized under this Agreement. The procedure for indemnification will be as set forth in the Section covering Customer's indemnification obligations.

7. Compliance.

7.1 ***Anti-Bribery & Corruption.*** Customer will not: (a) make any unlawful payments to any government official or employee; (b) make any unlawful payment to any person, or unlawfully provide anything of value (whether as property, services, or in any other form) to any person, for the purpose of obtaining an improper business advantage; or (c) agree, commit, or otherwise offer to undertake any of the foregoing actions in connection with this Agreement or any related activities.

7.2 ***International Trade Compliance.*** The sale, resale, or other disposition of Products and any related technology or documentation are subject to various economic sanctions, export control laws, and other restrictive trade measures administered by the U.S. and other applicable governments. Because these laws may have extraterritorial effect, Customer will comply with all such measures, where applicable, including, without limitation: (a) the Export Administration Act of 1979, as amended (50 U.S.C. §§ 2401–2420) and the Export Administration Regulations, 15 C.F.R. §§ 730–774 ("**EAR**"); (b) the Arms Export Control Act, 22 U.S.C. § 2778, and the corresponding Inter-

national Traffic in Arms Regulations ("**ITAR**"); (c) the economic sanctions laws and regulations enforced by the U.S. Department of the Treasury's Office of Foreign Assets Control ("**OFAC**"), 31 C.F.R. §§ 500, et seq., and the U.S. Department of State; and (d) the anti-boycott regulations, guidelines, and reporting requirements under the Export Administration Regulations and Section 999 of the Internal Revenue Service Code. Customer understands and acknowledges that it is solely responsible for complying with such laws whenever applicable. Customer further understands and acknowledges that it will not directly or indirectly export, import, sell, disclose, or otherwise transfer any Products to any country or party subject to such restrictions, and that it is solely responsible for obtaining any license(s) to export, re-export, or import the Products that may be required.

7.3 ***FOIA and Public Disclosure Requests.*** The purpose of the relationship between KnowBe4 and Customer is for Customer to purchase a subscription to the Products and Services that contain software, content, and information related to internet security awareness training, IT risk management, regulatory compliance, simulation of security attacks, vulnerability assessments, and other product and service offerings. The Products, Services, and any Confidential Information disclosed is proprietary to KnowBe4 and is an important business asset of KnowBe4 (the "**Proprietary Information**"). The Proprietary Information consists of protected financial data, trade secrets, and commercially valuable information that, if disclosed, would harm the competitive position of KnowBe4. In the event of a request for disclosure of KnowBe4's information, including any training materials, Customer will affirmatively respond denying the request pursuant to the terms of this paragraph and will promptly, but no later than five (5) business days after receiving such request, forward the request on to KnowBe4. Customer will not release any such information except pursuant to written instructions by KnowBe4, or a final un-appealable court order, provided that any such disclosure will be limited to the minimum necessary to be in compliance with the request, based upon the opinion of counsel. If Customer cannot agree to the foregoing, then Customer is not permitted access to the Proprietary Information.

7.4 ***Background Checks.*** In accordance with KnowBe4's background check policy for its US entity, and to the extent allowed by applicable laws, KnowBe4 has not knowingly employed any persons who, in the past seven (7) years, have been convicted of an offense involving violence, theft, fraud, money laundering, sex crimes, or other offenses that pose an unacceptable level of risk, given the scope of the applicable employment position and KnowBe4's business needs.

8. Product Support.

8.1 ***In General.*** Products are made available with standard Product Support for no additional charge. Customer may purchase priority level support for an additional fee as set

forth in the applicable Quote. Product Support is made available in accordance with the terms and conditions set forth in the SLA.

8.2 ***Exclusions.*** Notwithstanding the foregoing, KnowBe4 will have no obligation to support: (a) services, hardware, or software provided by anyone other than KnowBe4; (b) Product issues caused by Customer's negligence, abuse, or misapplication; or (c) Customer's use of Products other than as specified in the Documentation.

9. Payment Terms.

9.1 ***Prices.*** Prices will be specified by KnowBe4 and will be applicable for the period specified in the KnowBe4 Quote (as applicable). If no period is specified, prices will be applicable for thirty (30) calendar days. Notwithstanding the foregoing, prices may be subject to increase upon a renewal of a Quote, or in the event Customer adds-on or upgrades Products during the subscription term specified in the Quote. Prices are exclusive of taxes, including sales, use, excise, value added, and similar taxes or charges imposed by any government authority, and domestic and international shipping charges. KnowBe4 will identify on a separate line item on the applicable invoice, Quote, or order the taxes due on any Services supplied by KnowBe4 where KnowBe4 has established taxable nexus for all state and local transaction taxes (including sales, use, excise, withholding, or similar functional transaction level taxes, collectively, "**Transaction Level Taxes**"). In the event KnowBe4 does not include tax on an invoice to Customer, it will serve as notice to the Customer that KnowBe4 does not have taxable nexus for Transactional Level Taxes in the jurisdictions provided for by the Customer, and Customer will be responsible for calculating and remitting such Transaction Level Taxes, unless Customer provides KnowBe4 with a valid tax exemption certificate authorized by the appropriate taxing authority. Customer is not responsible for any taxes based on KnowBe4's income. Except as otherwise specified herein or in a Quote: (a) fees are based on the Product acquired and not actual usage; (b) payment obligations are non-cancelable and fees paid are non-refundable, except where expressly permitted herein; and (c) subscription term and quantities purchased cannot be decreased during the applicable subscription term. For clarity, Customer is responsible for any payments owed but not paid by any Affiliates ordering Products or Services hereunder.

9.2 ***Due Date; Late Payments.*** Amounts due for Products and Services may be invoiced by KnowBe4 in full at the start of the subscription term or as otherwise expressly provided in the Quote. Customer agrees to pay the net amount of each invoice without offset or deduction within thirty (30) days after the date of KnowBe4's invoice (unless otherwise noted on the invoice). If any undisputed amount is not paid by Customer within fifteen (15) days' notice of late payment, KnowBe4 will be entitled to receive the amount due plus interest thereon at a rate of 1.5% per month (or the highest rate permitted by applicable law) on all undisputed amounts that are not paid on or before the date due.

Customer will also pay all of KnowBe4's reasonable costs of collection including, but not limited to, reasonable attorneys' fees.

9.3 ***Disputed Payments.*** Customer has the right, in good faith, to dispute all or a portion of an invoice prior to its due date. KnowBe4 will not collect interest on disputed amounts in the event Customer provides KnowBe4 with written notice, prior to the due date, that Customer disputes such charges, pays all undisputed charges on time, and cooperates diligently to resolve the dispute.

9.4 ***Credit Approval; Application of Payment.*** All Quotes are subject to credit approval by KnowBe4. Customer agrees to submit such financial information from time to time as may be reasonably requested by KnowBe4 for the establishment and/or continuation of credit terms. Any payment received from Customer may be applied by KnowBe4 against any obligation owing from Customer to KnowBe4.

9.5 ***Channel Partner Purchases.*** In the event Customer acquires Products or Services via an authorized KnowBe4 channel partner (i.e., a reseller, distributor, managed service provider, etc.), all payment-related terms will be set forth in the applicable agreement between such channel partner and Customer.

10. Confidentiality.

10.1 ***Confidential Information.*** During the Term, each party may disclose to the other certain Confidential Information to the other party. Notwithstanding the foregoing, Confidential Information does not include information that: (a) is or becomes publicly available through no breach by the Receiving Party of this Agreement; (b) was previously known to the Receiving Party prior to the date of disclosure, as evidenced by contemporaneous written records; (c) was acquired from a third party without any breach of any obligation of confidentiality; (d) was independently developed by a party hereto without reference to Confidential Information of the other party; or (e) is required to be disclosed pursuant to a subpoena or other similar order of any court or government agency, provided, however, that the party receiving such subpoena or order will promptly inform the other party in writing and provide a copy thereof (unless notice is precluded by the applicable process), and will only disclose that Confidential Information necessary to comply with such subpoena or order.

10.2 ***Protection of Confidential Information.*** Except as expressly provided in this Agreement, the Receiving Party will not use or disclose any Confidential Information of the Disclosing Party without the Disclosing Party's prior written consent, except disclosure to, and subsequent uses by, the Receiving Party's employees or consultants on a need-to-know basis, provided that such employees or consultants have executed written agreements restricting use or disclosure of such Confidential Information that are at least as restrictive as the Receiving Party's obligations under this Section. Subject to the foregoing nondisclosure and non-use obligations, the Receiving Party will use at least the same degree of care and precaution that it uses to protect the confidentiality of

its own Confidential Information and trade secrets of similar nature, but in no event less than reasonable care. Each party acknowledges that due to the unique nature of the other party's Confidential Information, the Disclosing Party will not have an adequate remedy in money or damages in the event of any unauthorized use or disclosure of its Confidential Information. In addition to any other remedies that may be available in law, in equity, or otherwise, the Disclosing Party shall be entitled to seek injunctive relief to prevent such unauthorized use or disclosure.

10.3 ***Return and Destruction of Materials.*** All documents and other tangible objects containing or representing Confidential Information that have been disclosed by either party to the other party, and all summaries, copies, descriptions, excerpts, or extracts thereof that are in the possession of the other party will be, and remain, the property of the Disclosing Party and will be promptly returned to the Disclosing Party. The Receiving Party will use reasonable efforts to promptly delete or destroy all summaries, copies, descriptions, excerpts, or extracts thereof in their possession upon the Disclosing Party's written request. The Receiving Party will have no obligation to delete or destroy copies that: (a) are contained in an archived computer system backup that were made in accordance with such party's security, e-mail retention, and/or disaster recovery procedures; or (b) are kept by a party for record-keeping, archival, or governance purposes in compliance with such party's document retention policies. Any such retained Confidential Information will remain subject to the terms and conditions of this Agreement for so long as it is retained. Notwithstanding the return or destruction of the Confidential Information, the Receiving Party will continue to be bound by its confidentiality and other obligations hereunder in accordance with the terms of this Agreement. At the Disclosing Party's option, the Receiving Party will provide written certification of its compliance with this Section.

11. Warranties and Disclaimers.

11.1 ***Product Warranties.*** All purchased Products will materially conform to their then-current Documentation and during the applicable subscription term, KnowBe4 will not materially decrease the overall functionality of the Products. Customer must notify KnowBe4 of any breach of this warranty within thirty (30) days of discovery of the breach. Customer's sole and exclusive remedy, and KnowBe4's sole and exclusive liability, for a breach of the foregoing warranty, will be for KnowBe4 to provide Product Support to repair or replace the relevant Product within thirty (30) days of such notice of non-conformity. If KnowBe4 is unable to remedy such non-conformity within the period to cure, Customer will be entitled to terminate the relevant Quote and be issued a refund for any pre-paid, unearned fees for the affected portion of the Products. KnowBe4 will not be responsible for any breach of the foregoing warranty resulting from Customer's abuse or misuse of the Product or failure to use the Product as de-

scribed in this Agreement, including failure to use the Product in accordance with its operational requirements. Customer is required to sufficiently detail the non-conformity in a manner that allows KnowBe4 to properly assist with the remediation. KnowBe4 will not be responsible for delays in remediation caused by Customer's failure to respond to requests by KnowBe4. Customer understands that the Products will only operate in accordance with KnowBe4's Documentation, and it is Customer's responsibility to ensure that the Products will be fit for its purposes and to ensure that the Products will be supported by Customer's technology and business environment.

11.2 ***Service Warranties.*** KnowBe4 warrants that KnowBe4 will provide the Services in a professional, workmanlike manner consistent with this Agreement. Customer must notify KnowBe4 of any breach of this warranty within thirty (30) days of discovery of the breach. Customer's sole and exclusive remedy, and KnowBe4's sole and exclusive liability, for a breach of the foregoing warranty will be for KnowBe4, in its sole discretion, to use reasonable efforts to re-perform the Services or terminate the relevant Quote and issue a refund for the portion of pre-paid fees for the non-conforming Services.

11.3 ***Compliance Warranties.*** Each party warrants that it will comply with all laws and regulations applicable to its provision or use of the Products and Services, as applicable (including applicable security breach notification laws).

11.4 ***Disclaimers.*** EXCEPT FOR THE LIMITED WARRANTIES IN THIS SECTION: (A) THE PRODUCTS AND SERVICES ARE PROVIDED "AS IS," WITH ALL FAULTS, AND WITHOUT WARRANTIES OF ANY KIND; AND (B) KNOWBE4 EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, QUIET ENJOYMENT, QUALITY OF INFORMATION, TITLE, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. KNOWBE4 DOES NOT WARRANT THAT THE OPERATION OF THE PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE OR THAT DEFECTS IN THE PRODUCTS WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION, MARKETING, OR PROMOTIONAL MATERIALS, OR ADVICE GIVEN BY KNOWBE4 OR KNOWBE4'S AUTHORIZED REPRESENTATIVES WILL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THE EXPRESS WARRANTIES PROVIDED HEREIN. CUSTOMER ACKNOWLEDGES THAT COURSEWARE IS FOR GENERAL INFORMATION PURPOSES ONLY AND THAT KNOWBE4 IS NOT A LAW FIRM, NOR DOES IT PROVIDE ANY PROFESSIONAL OR ADVISORY SERVICES. THE INFORMATION PRESENTED IS NOT LEGAL ADVICE AND IS NOT TO BE ACTED ON AS SUCH. THE PRODUCTS MAY CONTAIN THE TRADE NAMES OR TRADEMARKS OF VARIOUS THIRD PARTIES AND, IF SO, ANY SUCH USE IS FOR ILLUSTRATIVE AND EDUCATIONAL PURPOSES ONLY. ALL PRODUCT AND COMPANY NAMES ARE PROPERTY OF THEIR RESPECTIVE OWNERS. USE OR DISPLAY OF THE MARKS DOES NOT IMPLY ANY AFFILIATION WITH, ENDORSEMENT BY, OR ASSOCIATION OF ANY KIND BETWEEN SUCH THIRD PARTIES AND KNOWBE4.

11.5 THE PRODUCTS AND SERVICES MAY BE USED TO ACCESS AND TRANSFER INFORMATION OVER THE INTERNET. CUSTOMER ACKNOWLEDGES AND AGREES THAT KNOWBE4 AND ITS VENDORS AND LICENSORS DO NOT OPERATE OR CONTROL THE INTERNET AND THAT: (A) VIRUSES, WORMS, TROJAN HORSES, OR OTHER UNDESIRABLE DATA OR SOFTWARE; OR (B) UNAUTHORIZED USERS (E.G., HACKERS) MAY ATTEMPT TO OBTAIN ACCESS TO, AND DAMAGE, CUSTOMER DATA, WEB-SITES, COMPUTERS, OR NETWORKS. KNOWBE4 WILL NOT BE RESPONSIBLE FOR THOSE ACTIVITIES. FURTHER, EACH PARTY DISCLAIMS ALL LIABILITY AND INDEMNIFICATION OBLIGATIONS FOR ANY HARM OR DAMAGES CAUSED BY ANY THIRD-PARTY HOSTING PROVIDERS.

12. Indemnification.

12.1 ***KnowBe4 Indemnity Obligations.*** KnowBe4 will defend and indemnify Customer from any and all claims, losses, deficiencies, damages, liabilities, costs, and expenses (including, but not limited to, reasonable attorneys' fees) finally awarded against Customer, as approved via a court-approved settlement, or via binding mediation or arbitration arising from a claim by a third party that Customer's authorized use of a Product infringes that third party's United States patent, copyright, or trade secret rights. The foregoing indemnification obligation of KnowBe4 is contingent upon Customer promptly notifying KnowBe4 in writing of such claim (provided the failure or delay in doing so will not relieve KnowBe4 from any obligations to indemnify Customer except to the extent that such delay or failure materially prejudices the defense of such claim), permitting KnowBe4 sole authority to control the defense or settlement of such claim and providing KnowBe4 reasonable assistance (at KnowBe4's sole expense) in connection therewith. If a claim of infringement under this Section occurs, or if KnowBe4 determines a claim is likely to occur, KnowBe4 will have the right, in its sole discretion, to either (a) procure for Customer the right or license to continue to use the Products free of the infringement claim; or (b) modify the Products to make them non-infringing, without loss of material functionality. If neither of these remedies is reasonably available to KnowBe4, KnowBe4 may, in its sole discretion, immediately terminate this Agreement and related Quote and, upon return of the infringing Products from Customer, provide a prorated refund for any prepaid, unused fees for such Products for the remainder of the applicable subscription Term. Notwithstanding the foregoing, KnowBe4 will have no obligation with respect to any claim of infringement that is based upon or arises out of: (a) the use or combination of the Products with any hardware, software, products, data, or other materials not provided by KnowBe4; (b) modification or alteration of the Products by anyone other than KnowBe4; (c) use of the Products in excess of the rights granted in this Agreement; or (d) any specifications or other intellectual property provided by Customer (collectively, the "**Excluded Claims**"). The provisions of this

Section state the sole and exclusive obligations and liability of KnowBe4 and its licensors and suppliers for any claim of intellectual property infringement arising out of or relating to the Products or this Agreement, and are in lieu of any implied warranties of non-infringement, all of which are expressly disclaimed.

12.2 ***Customer Indemnity Obligations.*** Customer will defend and indemnify KnowBe4 and hold it harmless from any and all claims, losses, deficiencies, damages, liabilities, costs, and expenses (including, but not limited to, reasonable attorneys' fees) incurred by KnowBe4 as a result of any claim by a third party arising from: (a) Customer's use of the Products in breach of this Agreement, (b) KnowBe4's authorized use of the Customer Data; or (c) the Excluded Claims. The foregoing indemnification obligation of Customer is contingent upon KnowBe4 promptly notifying Customer in writing of such claim (provided the failure or delay in doing so will not relieve Customer from any obligations to indemnify KnowBe4 except to the extent that such delay or failure materially prejudices the defense of such claim), permitting Customer sole authority to control the defense or settlement of such claim, provided that Customer may not settle any such claim unless it unconditionally releases KnowBe4 of all liability, and providing Customer reasonable assistance (at Customer's sole expense) in connection therewith.

13. Limitations of Liability.

13.1 NEITHER KNOWBE4 NOR ITS VENDORS OR LICENSORS WILL HAVE ANY LIABILITY TO CUSTOMER OR ANY THIRD PARTY FOR ANY LOSS OF PROFITS, SALES, BUSINESS, DATA, OR OTHER INCIDENTAL, CONSEQUENTIAL, OR SPECIAL LOSS OR DAMAGE, INCLUDING EXEMPLARY AND PUNITIVE DAMAGES, OF ANY KIND OR NATURE RESULTING FROM, OR ARISING OUT OF, THIS AGREEMENT, THE PRODUCTS, AND ANY SERVICES RENDERED HEREUNDER. THE TOTAL LIABILITY OF KNOWBE4 AND ITS VENDORS AND LICENSORS TO CUSTOMER OR ANY THIRD PARTY ARISING OUT OF THIS AGREEMENT, THE PRODUCTS, AND ANY SERVICES RENDERED HEREUNDER FOR ANY AND ALL CLAIMS OR TYPES OF DAMAGES WILL NOT EXCEED THE TOTAL FEES PAID OR PAYABLE HEREUNDER BY CUSTOMER FOR THE PRODUCT OR SERVICE AS TO WHICH THE LIABILITY RELATES, IN THE TWELVE (12) MONTHS PRIOR TO THE FIRST EVENT GIVING RISE TO LIABILITY. The allocations of liability in this Section represent the agreed, bargained-for understanding of the parties and KnowBe4's compensation hereunder reflects such allocations. The limitation of liability and types of damages stated in this Agreement are intended by the parties to apply, regardless of the form of lawsuit or claim a party may bring, whether in tort, contract, or otherwise, and regardless of whether any limited remedy provided for in this Agreement fails of its essential purpose.

14. Term and Termination.

14.1 ***Term.*** This Agreement will be effective as of the Effective Date and will remain in full force and effect until all Quote terms have expired or otherwise have been terminated ("**Term**").

14.2 ***Suspension.*** In the event KnowBe4, in good faith, believes or otherwise becomes aware of a User's violation of this Agreement, then KnowBe4 may specifically request that Customer suspend such User's access to, and use of, the Products. In the event Customer fails to suspend such non-compliant User, Customer hereby authorizes KnowBe4 to suspend such User. The duration of such suspension is at the sole determination of KnowBe4 and will continue until such time as KnowBe4 determines that the applicable User has cured the breach resulting in such suspension. KnowBe4 may also suspend access to, and use of, the Products with respect to any individual User or the Customer account to: (a) prevent damages to, or degradation of, the Products or KnowBe4's systems; (b) comply with any law, regulation, court order, or other governmental request; or (c) otherwise protect KnowBe4 from potential legal liability. Any such suspension will be to the minimum extent and of the minimum duration required to prevent or terminate the cause of the suspension.

14.3 ***Termination.***

14.3.1 If Customer fails to pay any invoice when due and does not make such payment within fifteen (15) days after receipt of notice from KnowBe4 of such failure, KnowBe4 may, in its sole discretion, either: (a) suspend delivery or performance of any Quote, or any remaining balance thereof, until such payment is made; or (b) terminate any Quote. In either event, Customer will remain liable to pay for the Products and Services.

14.3.2 Either party may terminate the Agreement or a Quote upon a material breach of the Agreement or Quote by the other, if the breaching party does not cure the breach within thirty (30) days after receipt of written notice from the other party specifying the breach.

14.3.3 Customer may terminate this Agreement or any applicable Quote at any time and for any reason upon providing thirty (30) days' written notice to KnowBe4, provided Customer will not be entitled to reimbursement or relief of its future payment obligations.

14.4 ***Effects of Termination.***

14.4.1 In the event of any termination of the Agreement or Quote without cause by Customer, or for cause by KnowBe4, Customer will pay for all Products and Services ordered as of the effective date of termination of the particular Quote. In addition, if a Quote specifies a term for which KnowBe4 will provide Products or Services to Customer (e.g., thirty-six (36) months), and that Quote is terminated by KnowBe4 for cause (including nonpayment) or by Customer without cause, then all future, recurring fees associated with the remaining term of such

Quote will become immediately due and payable, and will be paid by Customer to KnowBe4 upon the effective date of such termination.

14.4.2 Upon any termination, Customer's right to use and access the Products and Services (including any Courseware and other materials provided by KnowBe4) will immediately cease. Customer must return or destroy all copies (original and duplicates) of such Products and Services, in accordance with this Agreement. Upon request by KnowBe4, Customer must provide to KnowBe4 a certification of destruction.

14.4.3 During the applicable subscription term, Customer will have the ability to download a copy of its Customer Data contained in the Products in the form and format as such Customer Data exists in the Products. Upon termination of this Agreement or applicable subscription term, KnowBe4 will have the right to delete or destroy all Customer Data in KnowBe4, or in KnowBe4's agents' possession. Notwithstanding the forgoing, KnowBe4 will be permitted to retain copies of data contained in an archived computer system backup that: (a) was made in accordance with its security, e-mail retention, and/or disaster recovery procedures; or (b) are kept by KnowBe4 for record-keeping, archival, or governance purposes in compliance with KnowBe4's document retention policies. Any such retained data will remain subject to the provisions of this Agreement for so long as it is retained.

14.4.4 The exercise of the right to terminate this Agreement and any Quote will be in addition to any other rights or remedies provided in this Agreement, or existing at law or equity, that are not otherwise excluded or limited under this Agreement.

15. Miscellaneous Provisions.

15.1 ***U.S. Governmental Rights.*** The software Products and Services consist of commercial items and are commercial computer software as described in DFARS 252.227-7014(a)(1) and FAR 2.101. If acquired by or on behalf of any the Department of Defense or any component thereof, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of this Agreement as specified in DFARS 227.7202-3, Rights in Commercial Computer Software or Commercial Computer Software Documentation. If acquired by or on behalf of any civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of this Agreement as specified in FAR 12.212, Computer Software.

15.2 ***Insurance.*** KnowBe4 will maintain adequate insurance coverages as required by law or regulation, with an insurance carrier or carriers having an A.M. Best rating of A- or better, or an equivalent rating by another rating agency in the following amounts: (a) Comprehensive General Liability – not less than $1,000,000 per occurrence, $2,000,000

general aggregate; (b) Errors and Omissions (including Cyber & Privacy) – not less than $5,000,000 in the aggregate; and (c) Workers Compensation Coverage – as required by applicable law. Upon Customer's written request, KnowBe4 will furnish a Certificate of Insurance evidencing its insurance coverage to Customer.

15.3 ***Independent Contractor.*** KnowBe4, its personnel, agents, subcontractors and independent contractors are not employees or agents of Customer and are acting as independent contractors with respect to Customer. Neither party is, nor will be, considered to be an agent; distributor; partner; joint venture; or representative of the other party for any purpose, and neither party will have the authority to act on behalf of, or in the name of, or to bind, the other party in any manner whatsoever.

15.4 ***Force Majeure.*** Neither party to this Agreement will be liable for delays or failures in performance under this Agreement (other than the payment obligations or breach of confidentiality requirements) resulting from acts or events beyond the reasonable control of such party, including acts of war, terrorism, acts of God, natural disasters (fires, explosions, earthquakes, hurricane, flooding, storms, explosions, infestations), embargos, riots, sabotage, governmental acts, failure of the Internet, power failures, energy interruptions or shortages, other utility interruptions, or telecommunications interruptions, provided that the delayed party: (a) gives the other party notice of such cause without undue delay; and (b) uses its reasonable commercial efforts to promptly correct such failure or delay in performance.

15.5 ***Governing Law; Venue.*** The following provisions include the law that will apply in the event of any dispute or lawsuit arising out of or in connection with this Agreement, the courts that have jurisdiction over any such dispute or lawsuit, and the accompanying terms depend on where the Customer is domiciled in accordance with the following table. All proceedings to be conducted in English.

If the Customer is domiciled in:	**Without giving effect to any choice or conflict of law provisions, rules, or principles, the governing law is the laws of:**	**Courts with exclusive jurisdiction are:**	**Additional terms included are:**
A country in North America, Central America, South America or Caribbean, other than Brazil. If Customer is domiciled in Russia,	Florida and controlling United States federal law	Hillsborough County, Florida, U.S.A.	Notwithstanding the foregoing, the parties will have the right to seek injunctive or pre-judgment relief in any court of competent jurisdiction to prevent or enjoin the misappropriation, misuse, infringement or unauthorized disclosure of its Confidential Information or intellectual property rights. No Federal Acquisition Regulations will be construed to apply

or a geographic region that does not fall into one of the designations described in this table, then Customer will fall into this category.			to KnowBe4 without KnowBe4's written agreement thereto. The United Nations Convention for the International Sale of Goods will not apply to this Agreement. THE PARTIES HERETO WILL AND THEY HEREBY DO WAIVE TRIAL BY JURY IN ANY ACTION, PROCEEDING OR COUNTERCLAIM BROUGHT BY EITHER OF THE PARTIES HERETO AGAINST THE OTHER ON ANY MATTERS WHATSOEVER ARISING OUT OF OR IN ANY WAY RELATED TO THIS AGREEMENT.
A country in EMEA (Middle East, Europe and Africa) other than United Kingdom, South Africa, Germany, Austria and/or Switzerland	The Netherlands	Amsterdam	
Germany, Austria or Switzerland	Federal Republic of Germany	Berlin	The UN Convention on Contracts for the International Sale of Goods (UNCITRAL) will not apply.
United Kingdom	England and Wales	London	
Australia, New Zealand or Oceania	Victoria, Australia	Victoria, Australia	
Japan	Japan	Tokyo District Court	
Brazil	Federative Republic of Brazil	São Paulo, State of São Paulo, Brazil	The parties agree that any subpoena or notice relating to the proceeding will be made by registered correspondence.
South Africa	England and Wales	London	
A country in the Asia-Pacific region, other than Japan, Australia, New Zealand or Oceania	Singapore	Singapore	

15.6 This Agreement, including any and all Quotes, constitutes the entire understanding between the parties related to this Agreement which understanding supersedes and merges all prior understandings and all other proposals, letters, agreements, whether oral or written. The parties further agree that there are no other inducements, warranties, representations, or agreements regarding the matters herein between the parties except as expressly set forth in this Agreement. In the event of any conflict between the body of this Agreement and any Quote, or additional agreements entered into by the parties, the body of this Agreement will control, unless otherwise expressly stated in a signed writing by authorized representatives of the parties. In the event that the Customer or Users are presented with KnowBe4 click-wrap, the contents of this Agreement will supersede any conflicting terms. As used herein, the term "including" will mean "including, without limitation"; the term "includes" as used herein will mean "includes, without limitation"; and terms appearing in the singular will include the plural, and terms appearing in the plural will include the singular. This Agreement may not be modified, amended, or altered in any manner except by a written agreement signed by authorized representatives of the parties, and any attempt at oral modification will be void and of no effect.

15.7 ***Assignment.*** This Agreement may not be assigned or transferred by either party without the prior written consent of the other party, which consent will not be unreasonably withheld, conditioned, or delayed. Notwithstanding the foregoing, either party may assign its rights and obligations under this Agreement, in whole but not in part, without the other party's permission, to an Affiliate (provided previously purchased licenses, access rights, and Seats for the Products and Services will not be assignable or transferable without written consent from KnowBe4) or in connection with any merger, consolidation, sale of all or substantially all of such assigning party's assets, or any other similar transaction, provided, that the assignee: (a) is not a direct competitor of the non-assigning party; (b) is capable of fully performing the obligations of the assignor under this Agreement; and (c) agrees to be bound by the provisions of this Agreement.

15.8 ***No Waiver.*** The waiver or failure of either party to exercise any right in any respect provided for herein will not be deemed to be a waiver of any further right.

15.9 ***Purchase Order***. KNOWBE4 SPECIFICALLY OBJECTS TO ANY ADDITIONAL TERMS BEING ADDED THROUGH A CUSTOMER PROVIDED PURCHASE ORDER OR SIMILAR DOCUMENT. IF A PURCHASE ORDER IS REQUIRED BY CUSTOMER, THE PARTIES AGREE THAT ANY ADDITIONAL TERMS CONTAINED THEREIN WILL NOT BECOME PART OF THE AGREEMENT BETWEEN THE PARTIES AND, SPECIFICALLY, THAT THE TERMS OF THIS AGREEMENT WILL SUPERSEDE AND REPLACE ANY AND ALL TERMS IN ANY PURCHASE ORDER.

15.10 ***Survivability.*** All provisions of this Agreement relating to confidentiality, non-disclosure, intellectual property, disclaimers, limitation of liability, indemnification, payment, and

any other provisions which must survive in order to give effect to their meaning will survive the termination of this Agreement.

15.11 ***Severability.*** If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision will be deemed null and void, and the remaining provisions of this Agreement will remain in effect.

15.12 ***Notices.*** Except as otherwise specified in this Agreement, all notices related to this Agreement will be in writing and will be effective upon (a) personal delivery, (b) the third business day after mailing, or (c) the day of sending by email. All notices from Customer pertaining to contractual or legal matters (i.e. breach of contract, termination, indemnifiable claims, etc.) must clearly be identified and marked as Legal Notices to the address listed below. Billing-related notices to Customer will be addressed to the relevant billing contact designated by Customer. All other notices to Customer will be addressed to the relevant account administrator designated by Customer.

Notice address for KnowBe4:

KnowBe4, Inc.

Attn: Legal Department

33 N. Garden Ave.

Suite 1200

Clearwater, Florida, U.S.A. 33755

support@knowbe4.com

15.13 ***Headings; Counterparts; Electronic Signatures.*** The headings contained in this Agreement are for purposes of convenience only and shall not affect the meaning or interpretation of this Agreement. This Agreement may be executed in two or more original or facsimile counterparts, each of which will be deemed an original, but all of which together shall constitute one and the same instrument. The parties agree that the electronic signature of a party to this Agreement shall be as valid as an original signature of such party and shall be effective to bind such party to this Agreement. The parties agree that any electronically signed document (including this Agreement) shall be deemed (i) to be "written" or "in writing," (ii) to have been signed and (iii) to constitute a record established and maintained in the ordinary course of business and an original written record when printed from electronic files. Such paper copies or "printouts," if introduced as evidence in any judicial, arbitral, mediation or administrative proceeding,

will be admissible as between the parties to the same extent and under the same conditions as other original business records created and maintained in documentary form. For purposes hereof, "electronic signature" means a manually-signed original signature that is then transmitted by electronic means; "transmitted by electronic means" means sent in the form of a facsimile or sent via the internet as a "pdf" (portable document format) or other replicating image attached to an e-mail message; and, "electronically signed document" means a document transmitted by electronic means and containing, or to which there is affixed, an electronic signature.

16. Country Specific Provisions. The following provisions are specific to the local law requirements for the specific country indicated, only.

16.1 ***Local Law Requirements for Japan.*** If Customer is domiciled in Japan, then Customer represents and warrants that it, and it officers, directors, and material shareholders, are not: (a) Anti-Social Forces (defined below), and have not been for at least the last five years; and (b) involved with Anti-Social Forces, including, without limitation, involvement by management, utilization, or provision of funding or favors. KnowBe4 may immediately terminate this Agreement for cause in the event of a breach of any of these representations and warranties. For the purposes of this section "Anti-Social Forces" means, collectively, an organized crime group (bouryokudan) or a member or affiliate thereof, a corporate racketeer (soukaiya), a rogue person or group advocating a social or political movement, or any other anti-social forces.

16.2 ***Local Law Requirements for Germany.*** With respect to Customers domiciled in Germany, Section 13 "Limitation of Liability" of this Agreement is replaced with the following:

"13 Limitation of Liability for Customers Domiciled in Germany.

13.1 ***Unlimited Liability.*** The Parties will be mutually liable without limitation: (a) in the event of willful misconduct or gross negligence; (b) within the scope of a guarantee taken over by the respective party; (c) in the event that a defect is maliciously concealed; (d) in case of an injury to life, body or health; or (e) according to the German Product Liability Law.

13.2 ***Liability for Breach of Cardinal Duties.*** If cardinal duties are infringed due to slight negligence and if, as a consequence, the achievement of the objective of this Agreement including any applicable Quote is endangered, or in the case of a slightly negligent failure to comply with duties, the very discharge of which is an essential prerequisite for the proper performance of this Agreement (including any applicable Quote), the parties' liability will be limited to foreseeable damage typical for the contract. In all other respects, any liability for damage caused by slight negligence will be excluded.

13.3 Unless the parties are liable in accordance with "Unlimited Liability" section above, in no event will the aggregate liability of each party together with all of its Affiliates arising out of or related to this Agreement exceed the total amount paid by Customer and its Affiliates hereunder for the Services giving rise to the liability in the 12 months preceding the first incident out of which the liability arose. The foregoing limitation will not limit Customer's and its Affiliates' payment obligations.

13.4 With the exception of liability in accordance with the "Unlimited Liability" section, the above limitations of liability will apply to all claims for damages, irrespective of the legal basis including claims for tort damages. The above limitations of liability also apply in the case of claims for a party's damages against the respective other party's employees, agents or bodies.

13.5 Any rights arising out of or in connection with this Agreement will expire 24 months after the beginning of the statutory limitation period. The statutory limitation rules for intentional and grossly negligent acts, for claims due to intentional or negligent injury to life, body or health, for fraudulent misrepresentation and for claims under the Product Liability Act as well as sec. 548 of the German Civil Code will remain unaffected.

SERVICE LEVEL AGREEMENT

This Service Level Agreement ("SLA") is for the provisioning of services required to support and sustain the Products under the Agreement to which this SLA is attached.

Term

This SLA is valid for the subscription term specified in the applicable Quote. Termination of the Agreement and/or a Quote will result in termination of this SLA.

Availability & Uptime

KnowBe4 agrees to: (a) make the Products available to Customer pursuant to the Agreement and the applicable Quote, (b) provide support for the Products to Customer at no additional charge, and/or upgraded support if purchased; and (c) use commercially reasonable efforts to make the online Services available 99.9% of the time to be measured annually, excluding any planned downtime, maintenance windows, or any unavailability caused by circumstances beyond KnowBe4's reasonable control, such as a force majeure event in accordance with the Agreement. If Customer would like to receive status updates on the availability of KnowBe4's Products, Customer may subscribe to receive updates at https://status.knowbe4.com/, or such other URL as KnowBe4 may provide from time to time.

CSM

Customer will be assigned a designated customer service manager ("**CSM**") to assist the Customer's admin with onboarding and training on how to use the Products, as applicable.

Maintenance Windows

Maintenance windows for other Products not specified below may be found on the KnowBe4 Documentation page, as defined in the Agreement.

- **KMSAT** maintenance windows may be found at https://support.knowbe4.com/hc/en-us/articles/360024057834-KnowBe4-Security-Awareness-Training-KMSAT-Site-Maintenance-, or such other URL as KnowBe4 may provide from time to time.
- **KCM GRC** maintenance windows may be found at https://support.knowbe4.com/hc/en-us/articles/360025164193-KCM-GRC-Platform-Maintenance-Window, or such other URL as KnowBe4 may provide from time to time.
- **PhishER** maintenance windows may be found at https://support.knowbe4.com/hc/en-us/articles/360025164473-PhishER-Platform-Site-Maintenance-, or such other URL as KnowBe4 may provide from time to time.

Support

KnowBe4's support parameters, including its support hours, may be found at https://www.knowbe4.com/hubfs/KnowBe4-Support-Document.pdf?t=1518625292505, or such other URL as KnowBe4 may provide from time to time. To make a support request, Customer may

submit a ticket at https://support.knowbe4.com/hc/en-us/requests/new, or such other URL as KnowBe4 may provide from time to time.

Customer Requirements

Customer responsibilities and/or requirements in support of this SLA include: (a) Customer's compliance with the Agreement and the applicable Quote; (b) reasonable availability of Customer's admin and/or technical representative(s) when resolving a service-related incident or request; and (c) providing proper notice of KnowBe4's non-compliance with any Product or Service warranty in accordance with the Agreement and sufficiently detailing the non-compliance in a manner that enables KnowBe4 to properly assist with the remediation. KnowBe4 will not be responsible for delays in remediation caused by Customer's failure to respond to requests by KnowBe4. Customer understands that the Products and Services will only operate in accordance with KnowBe4's Documentation, as defined in the Agreement, and it is Customer's responsibility to ensure that the Products and Services will be fit for its purposes and to ensure that the Products and Services will be supported by Customer's technology and business environment. Customer understands that KnowBe4's Products and Services are non-mission critical to Customer's business.

Response Times

In support of services outlined in this SLA, KnowBe4 will respond to service-related incidents and/or requests submitted by Customer within the following time frames:

- Within 2 business days for issues classified as **High Priority**.
    - "**High Priority**": Complete failure of platform or the complete unavailability of core functionality such as training and phishing.
- Within 3 business days for issues classified as **Medium Priority**.
    - "**Medium Priority**": Impacted operations, core operations such as user and admin login operational but functionality impaired or requiring workarounds to achieve documented operation.
- Within 5 business days for issues classified as **Low Priority**.
    - "**Low Priority**": Inconvenience due to operations not performing as defined or at a significantly degraded speed.

KMSAT Support Tiers

Tier 1 Support will assist with:

- Password resets
- Phishing and Training Campaign creation
- Explaining overall navigation of the KMSAT Products
- Providing KnowBe4's recommended best practices
- Issues accessing the training console
- Whitelisting to ensure successful delivery of email from our servers
- Issues related to accessing/completion of training modules
- Resolving phishing/training result discrepancies
- SAML Single Sign-On support and troubleshooting
- Phish Alert Button installation
- Active Directory Integration support
- Channel partner support

Tier 2 and Tier 3 Support will be available for the escalation of more advanced support requests related to issues occurring with the KMSAT Products.

Channel Partners

In the event Customer purchases through a KnowBe4-authorized channel partner, such channel partner may have its own SLA associated with the purchase. Customer acknowledges that KnowBe4 is not responsible, nor is KnowBe4 liable, for ensuring compliance with such channel partner SLA.

INFORMATION SECURITY REQUIREMENTS

1. **Security.**
   a. KnowBe4 will maintain Customer Confidential Information and its information technology environment secure from unauthorized access by using commercially reasonable efforts and industry standard organizational, physical and technical safeguards, and refrain from implementing changes that materially lower the level of security protection provided as of the Effective Date of the Agreement. KnowBe4 will comply with the minimum security standards set forth in this Exhibit and provide prior written notice to Customer of any significant changes to KnowBe4's information security policy that would lessen the security posture of the environment.
   b. KnowBe4 will conduct a SOC-2 Type 2 or such similar or successor audit on an annual basis. Upon request, KnowBe4 will provide Customer with a copy of such audit report and promptly remediate and/or mitigate any non-conformance findings in like with KnowBe4's existing vulnerability remediation process. Such audit report will be considered Confidential Information of KnowBe4.
2. **Audit Rights.** Not more than once per calendar year during the term of the Agreement and with at least thirty (30) days' prior written notice by Customer to KnowBe4, Customer may, at Customer's sole expense, audit KnowBe4 to verify compliance with the terms and conditions of this Exhibit. Such audit will be:
   a. Completed within two (2) weeks;
   b. Performed during KnowBe4's regular business hours in a manner that, in KnowBe4's reasonable judgment, does not disrupt or degrade KnowBe4's regular business operations and is done in accordance with KnowBe4's security and data protection policies;
   c. Limited to KnowBe4's facilities and personnel of KnowBe4 in scope of this Agreement; and
   d. Conducted by either Customer's employees or, with KnowBe4's approval, by an independent third party agreed to by the parties.

   Customer may create an audit report summarizing the findings and observations of the audit ("Audit Report"). Audit Reports are deemed to be Confidential Information of KnowBe4 and the Customer will not disclose the Audit Reports to third parties except to Customer's legal counsel and consultants bound by obligations of confidentiality using at least the same degree of care Customer employs in maintaining in confidence its own Confidential Information of a similar nature, but in no event less than a reasonable degree of care. Customer will disclose the results of its audit to KnowBe4 within one week after its completion. KnowBe4 will promptly respond to audit findings and, at KnowBe4's expense,

discuss the findings with Customer, and if applicable, remediate and/or mitigate any critical and high risk findings to the satisfaction of Customer.

3. **Technical Security Controls.** With respect to KnowBe4 infrastructure that processes, stores, or transmits Customer Confidential Information, KnowBe4 will use the following technical security controls where applicable (and keep them current by incorporating and using all updates commercially available):

   a. Network Protection

      (i) Network based firewalls or equivalent

      (ii) Network intrusion detection/protection systems

   b. Client Protection

      (i) An antivirus or endpoint protection program using software that is updated at least daily on all applicable systems that may store or process Customer Confidential Information

      (ii) Host-based firewall/intrusion prevention software that blocks activity not directly related to or useful for business purposes

   c. System and Software Protection

      (i) All system and applications must utilize secure authentication and authorization mechanisms

      (ii) All KnowBe4-developed applications must be designed and implemented using secure coding standards and design principles (e.g., OWASP)

      (iii) Operating systems must be hardened appropriately according to industry standard practices

      (iv) Systems must be inspected for known vulnerabilities and all identified known vulnerabilities must be patched as soon as reasonably possible

   d. Encryption

      (i) KnowBe4 will review and update encryption configurations on all systems that utilize encryption. KnowBe4 will utilize only modern industry accepted encryption algorithms, ciphers, modes and key sizes

   e. Customer Confidential Information Protection

      (i) Customer Confidential Information Access: KnowBe4 will ensure that only authorized individuals (based on role) will, on behalf of KnowBe4, have access to Customer Confidential Information

      (ii) Customer Confidential Information Storage: KnowBe4 will not process Customer Confidential Information on or transfer such to any portable storage medium, unless the storage medium is fully encrypted in accordance with encryption requirements set forth in this Exhibit

      (iii) Customer Confidential Information Transmission: All transmission or exchange of Customer Confidential Information by Company will use secure protocol standards in accordance with encryption requirements set forth in this Exhibit

4. **Incidents.**

   a. If KnowBe4 becomes aware of any unauthorized access to the Customer Confidential Information on systems owned, managed, or subcontracted by KnowBe4, KnowBe4 will without undue delay, notify Customer; consult and reasonably cooperate with investigations and potentially required notices; and provide any information reasonably requested by Customer

   b. In the event of a breach or any unauthorized disclosure of Customer Confidential Information, at no additional cost to Customer, KnowBe4 will reasonably cooperate with Customer in investigating the incident including, but not limited to, the provision of system, application, and access logs, conducting forensics reviews of relevant systems, imaging relevant media, and making personnel available for interview

   c. On notice of any actual breach, KnowBe4 will immediately institute appropriate controls to maintain and preserve all electronic evidence relating to the breach in accordance with industry standard practices

5. **Integration.** The terms of this Exhibit apply in addition to, not in lieu of, any other terms and conditions agreed with KnowBe4, except as specifically and expressly agreed in writing with explicit reference to this Exhibit.

6. **Training.** KnowBe4 will periodically provide those employees, consultants, and any approved third parties (affiliated or not) that manage, or have access to, Confidential Information, including personally identifiable information, provided or made available by Customer, with privacy and security awareness training.