Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Order Form

CALL OFF CONTRACT REFERENCE: WP2153

CALL OFF CONTRACT TITLE: DevOps Support

CALL OFF CONTRACT DESCRIPTION: Provision of DevOps capability to support the delivery of the GOV.UK One Login digital identity solution.

THE BUYER: Government Digital Service on behalf of Cabinet Office

BUYER ADDRESS:

Cabinet Office Main Address: REDACTED

GDS Main Address: REDACTED

THE SUPPLIER: Capgemini UK Plc

SUPPLIER ADDRESS: REDACTED

REGISTRATION NUMBER: REDACTED **DUNS NUMBER:** REDACTED

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and is dated 7th August 2023.

It's issued under the Framework Contract with the reference number RM6263 for the provision of Digital Specialists and Programmes Deliverables.

The Parties intend that this Call-Off Contract will not, except for the first and subsequent Statement of Work's, oblige the Buyer to buy or the Supplier to supply

Deliverables.

The Parties agree that when a Buyer seeks further Deliverables from the Supplier under the Call-Off Contract, the Buyer and Supplier will agree and execute a further Statement of Work (in the form of the template set out in Annex 1 to this Framework Schedule 6 (Order Form Template, SOW Template and Call-Off Schedules).

Upon the execution of each Statement of Work it shall become incorporated into the Buyer and Supplier's Call-Off Contract.

CALL-OFF LOT(S):
RM6263 - Lot 1 Digital Programmes

CALL-OFF INCORPORATED TERMS
The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form, including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1 (Definitions) RM6263
3. Framework Special Terms

The following Schedules in equal order of precedence:

Joint Schedules for RM6263

- Joint Schedule 2 (Variation Form)
- Joint Schedule 3 (Insurance Requirements)
- Joint Schedule 4 (Commercially Sensitive Information)
- Joint Schedule 5 (Corporate Social Responsibility)
- Joint Schedule 6 (Key Subcontractors) - NOT USED
- Joint Schedule 7 (Financial Difficulties) - NOT USED
- Joint Schedule 8 (Guarantee) - NOT USED
- Joint Schedule 9 (Commercially Sensitive Information)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)
- Joint Schedule 12 (Supply Chain Visibility) - NOT USED
- Joint Schedule 13 (Cyber Essentials Scheme)

Call-Off Schedules for RM6263

- Call-Off Schedule 1 (Transparency Reports)
- Call-Off Schedule 2 (Staff Transfer)
- Call-Off Schedule 3 (Continuous Improvement)
- Call-Off Schedule 4 (Call Off Tender)
- Call-Off Schedule 5 (Pricing Details and Expenses Policy)
- Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliveries)

- Call-Off Schedule 7 (Key Supplier Staff)
- Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
- Call-Off Schedule 9 (Security) - NOT USED
- Call-Off Schedule 10 (Exit Management)
- Call-Off Schedule 12 (Clustering) - NOT USED
- Call-Off Schedule 13 (Implementation Plan and Testing)
- Call-Off Schedule 14B (Service Levels and Balanced Scorecard)
- Call-Off Schedule 15 (Call-Off Contract Management)
- Call-Off Schedule 16 (Benchmarking) - NOT USED
- Call-Off Schedule 18 (Background Checks)
- Call-Off Schedule 20 (Call-Off Specification)
- Call-Off Schedule 25 (Ethical Walls Agreement)
- Call-Off Schedule 26 (Secondment Agreement Template)

4. CCS Core Terms (version 3.0.11)
5. Joint Schedule 5 (Corporate Social Responsibility) RM6263
6. Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS AND SCHEDULES
The following Special Terms and Schedules are incorporated into this Call-Off Contract:

Security

1. The Supplier shall engage and collaborate with GDS Security Working Group reviews led by Digital Identity security leads.
2. The Supplier shall comply with Call Off Special Schedule 2 (Security Schedule for Development). For the purposes of that schedule this Contract is a “higher risk agreement”.

Data Protection

3. Paragraph 6(d) of Joint Schedule 11 shall be replaced with the following paragraph :

“*(d) not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:*

(i) the destination country has been recognised as adequate by the UK government in accordance with Article 45 UK GDPR or section 74 of the DPA 2018;

*(**ii**) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 DPA 2018) as determined by the Controller;*

(iii) the Data Subject has enforceable rights and effective legal remedies;

(iv) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

(v) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and"

Staff Vetting

4. The Supplier shall comply and ensure that its subcontractors other than Cloud Service Providers ("Non-CSP subcontractors") comply with the following procedures with respect to the vetting of all staff engaged by the Supplier or its Non-CSP subcontractors in the delivery of the Services ("Supplier Staff")

5. Subject to paragraphs 3 to 5 the Supplier shall ensure that:
   a. all Supplier Staff who are required to have to have security, architect development, coding or production platform access shall have passed SC clearance unless otherwise agreed by the Buyer; and
   b. all other Supplier Staff who are engaged in the delivery of the Services shall have passed BPSS clearance unless otherwise agreed by the Buyer.
6. The Supplier will be deemed to be in compliance with paragraph 2 where the Supplier (or its Non-CSP subcontractor where applicable) has submitted an application for the necessary clearance prior to the relevant member of the Supplier Staff being assigned to the delivery of the Services PROVIDED THAT:
   a. the Supplier shall immediately notify the Buyer if a member of the Supplier Staff has been refused the relevant clearance; and
   b. the Supplier shall immediately remove the relevant person from the delivery of the Services, if instructed to do so by the Buyer.
7. The Supplier shall ensure that all Supplier Staff are UK based unless otherwise agreed by the Buyer in accordance with this paragraph: a. the Buyer is entitled to refuse to allow Supplier Staff to be based in any country the laws, practices or policies of which the Buyer (in its absolute discretion) considers to pose a potential threat to the Buyer or its business;
   b. Where the Supplier wishes to engage Supplier Staff who are located in another country, the Supplier must seek authority and permission from the Buyer who will have absolute discretion in this circumstances. A risk assessment will need to be undertaken by the Buyer as to the impacts which may arise. Where it is agreed, the Supplier will need to demonstrate and evidence vetting checks in parallel/comparative to that required for BPSS checks in the UK. SC clearance is not available to outside UK resources.
8. **Exceptions Process**. Notwithstanding paragraphs 4 to 7, the Buyer reserves the right (in its absolute discretion) to approve the appointment of any member of Supplier Staff taking account of such investigations or considerations as the Buyer's

Information Assurance function sees fit to carry out or deems relevant.

9. The Supplier shall ensure that all records of vetting checks are accessible either via a certificated BPSS/SC document for the individual or in the form of a documented checklist. The Supplier must maintain records of all such checks and make them available to the Buyer for audit purposes on request.

Collaboration with other suppliers to the One Login Programme

10. If required by the Buyer, the Supplier shall enter into a Collaboration Agreement between the Buyer, the Supplier and such other suppliers to the Buyer's One Login Programme as the Buyer may require. The Collaboration Agreement shall be substantially in the form set out in Call Off Special Schedule 1.

11. In addition to any obligations under the Collaboration Agreement, the Supplier must:
    a. work proactively and in good faith with each of the Buyer's suppliers

    b. co-operate and share information with the Buyer's suppliers to enable the efficient delivery of the Buyer's One Login Programme.

Ethical Walls Agreement

12. The Supplier shall provide a signed copy of an Ethical Walls Agreement substantially in the form set out in Call Off Schedule 25 within 14 days of the Call Off Start Date or such longer period as the Buyer may determine.

CALL-OFF START DATE:	**7th August 2023**
CALL-OFF EXPIRY DATE:	**6th August 2025**
CALL-OFF INITIAL PERIOD:	**2 years**
CALL-OFF OPTIONAL EXTENSION PERIOD:	**6 months**
MINIMUM NOTICE PERIOD FOR EXTENSION(S):	**3 months**
CALL-OFF CONTRACT VALUE:	**Up to £8,000,000**
KEY SUB-CONTRACT PRICE:	**N/A**

CALL-OFF DELIVERABLES

Suppliers will be required to deliver the roles outlined in Attachment 3 and the Deliverables agreed in any Statements of Work.

BUYER's STANDARDS

From the Start Date of this Call-Off Contract, the Supplier shall comply with the relevant (and current as of the Call-Off Start Date) Standards set out in Framework Schedule 1 (Specification). The Buyer requires the Supplier to comply with the following additional Standards for this Call-Off Contract:

The Buyer requires the Supplier to comply with the following additional Standards:

- The Services must be delivered as per the GDS Service Manual (e.g. agile delivery aligned to scrum methodology) or other methodologies as required.

- The supplier should follow where applicable:
  - The Government Technology Code of Practice (https://www.gov.uk/government/publications/technology-code-of-practice)
  - The Government Service Standard and Service Manual (https://www.gov.uk/service-manual/service-standard)
  - Resources to be supplied in accordance with DDAT Competency framework guidelines: https://www.gov.uk/government/collections/digital-data-and-technology-profession-capability-framework
  - NCSC Cyber Assessment Framework Guidance https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework
  - NCSC guidance https://www.ncsc.gov.uk/section/advice-guidance/all-topics
  - ISO 270001

- The Supplier shall identify any conflicts of interest and, where identified, shall inform
the Buyer of such conflicts of interest and how they plan to mitigate the risk.
- Deliverables are to be Tested and accepted in line with the criteria set out in the applicable SoW.
- Agreeing a Statement of Work
  - Buyer to draft SOW with milestone deliverables for the outcome
  - Buyer Project Lead and Buyer Contracts Manager discuss SOW with Supplier
  - Supplier to propose the team required to deliver the outcome.
  - Supplier will share costs, timelines and team profile
  - Buyer to agree the team proposed
  - SOW is signed

CYBER ESSENTIALS SCHEME

The Buyer requires the Supplier, in accordance with Joint Schedule 13 (Cyber Essentials Scheme) to provide a Cyber Essentials Plus Certificate prior to commencing the provision of any Deliverables under this Call-Off Contract.

MAXIMUM LIABILITY

Each Party's total aggregate liability in each Contract Year for this Call-Off Contract under clause 11.2 of the Core Terms is no more than the greater of £4 million or 150% of the Estimated Yearly Charges.

CALL-OFF CHARGES

(1) Capped Time and Materials (CTM). The Contract will have a capped value of £8 million. The Buyer will have an option to terminate when the contract value reaches £5 million.

See Call-Off Schedule 5 (Pricing Details and Expenses Policy) for further details.

The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of:

- Specific Change in Law

Where non-UK Supplier Staff (including Subcontractors) are used to provide any element of the Deliverables under this Call-Off Contract, the applicable rate card(s) shall be incorporated into Call-Off Schedule 5 (Pricing Details and Expenses Policy) and the Supplier shall, under each SOW, charge the Buyer a rate no greater than those set out in the applicable rate card for the Supplier Staff undertaking that element of work on the Deliverables.

REIMBURSABLE EXPENSES
N/A.

PAYMENT METHOD
The Supplier will issue valid electronic invoices monthly in arrears. Each invoice shall be accompanied by a breakdown of the deliverables and services, quantity thereof, applicable unit charges and total charge for the invoice period, in sufficient detail to enable the Buyer to validate the invoice. Please ensure the invoice has the PO number and WP2141.

The Supplier will send reporting data via .CSV file as well as the PDF invoice so invoices can be automatically reconciled by GDS systems - see CSV template attached to the email.

Invoices to be sent to:

PDF Invoices and .CSV reports will be sent to:

REDACTED

which is at Cabinet Office,

REDACTED

BUYER'S INVOICE ADDRESS:

REDACTED

REDACTED

BUYER'S AUTHORISED REPRESENTATIVE

REDACTED

BUYER'S ENVIRONMENTAL POLICY
Please find below the link to the GDS sustainable development

policy:

https://intranet.cabinetoffice.gov.uk/task/sustainable-development/

BUYER'S SECURITY POLICY
See Call Off Special Clause 2.

SUPPLIER'S AUTHORISED REPRESENTATIVE

REDACTED

SUPPLIER'S CONTRACT MANAGER

REDACTED

PROGRESS REPORT FREQUENCY
On the first Working Day of each calendar month, unless otherwise agreed between both Parties.

PROGRESS MEETING FREQUENCY
Monthly on the first Working Day of each month unless otherwise agreed between both Parties.

KEY STAFF

REDACTED

TUPE

In Call Off Schedule 2 (Staff Transfer), parts C and E only shall apply.

KEY SUBCONTRACTOR(S)
N/A

COMMERCIALLY SENSITIVE INFORMATION

- REDACTED

MATERIAL KPIs
The following Material KPIs shall apply to this Call-Off Contract in accordance with Call-Off Schedule 14B (Service Levels and Balanced Scorecard):

KPI 1: Delivery of key milestones within agreed timescales as required by the Buyer and set out in the Statement of Works (SoW).

KPI 2: Delivery of code to DoD Standards (to be issued by the Buyer upon contract commencement) within agreed timescales set by the Buyer for this piece of work.

KPI 3: The Supplier shall provide suitable staff substitutions within 5 Working Days where required.

KPI 4: Management Information Reports must be received within agreed reporting timescales and must contain links to data sources.

KPI 5: Partnering behaviours and added value and knowledge share

Supplier promotes positive collaborative working relationships, within and across the team, by acting in a transparent manner. Supplier shows commitment to Buyer goals through adding value over and above and knowledge sharing and upskilling of GDS staff

KPI 6: Team in place (Delivery)

All Supplier resources proposed and Supplier resources already delivering the services have the skill-set and experience required to deliver the outcome. The contracts are therefore performing to the expected standard and deliverables are being met.

KPI 7: Knowledge Transfer and Capability Building.

Supplier works closely with the Buyer to jointly design and deliver a programme of repeatable activities and work streams to identify and build the Contracting Authority's capability across DDaT skills and at different levels of seniority and experience.

ADDITIONAL INSURANCES
Additional Insurances required in accordance with Joint Schedule 3 (Insurance Requirements): Global Public and Products Liability Insurance with a minimum level of indemnity of £5 million.

GUARANTEE
N/A

SOCIAL VALUE COMMITMENT

The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender)

STATEMENT OF WORKS

During the Call-Off Contract Period, the Buyer and Supplier may agree and execute completed Statement of Works. Upon execution of a Statement of Work the provisions detailed therein shall be incorporated into the Call-Off Contract to which this Order Form relates.

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:		**Signature:**	

Name:		**Name:**	
Role:		**Role:**	
Date:		**Date:**	

Appendix 1

Annex 1 (Template Statement of Work)

Statement of Work 1 will be signed between the Buyer and Supplier following execution of this Call-Off Contract.

1. STATEMENT OF WORK ("SOW") DETAILS	
The Parties will execute a SOW for each set of Buyer Deliverables required. Any ad-hoc Deliverables requirements are to be treated as individual requirements in their own right and the Parties should execute a separate SOW in respect of each, or alternatively agree a Variation to an existing SOW. **All SOWs must fall within the Specification and provisions of the Call-Off Contact.** **The details set out within this SOW apply only in relation to the Deliverables detailed herein and will not apply to any other SOWs executed or to be executed under this Call-Off Contract, unless otherwise agreed by the Parties in writing.**	
Date of SOW:	
SOW Title:	
SOW Reference:	
Call-Off Contract Reference:	
Buyer:	
Supplier:	
SOW Start Date:	
SOW End Date:	

Duration of SOW:	
Key Personnel (Buyer)	
Key Personnel (Supplier)	
Subcontractors	

2. CALL-OFF CONTRACT SPECIFICATION - PROGRAMME CONTEXT

SOW Deliverables Background

[Insert details of which elements of the Deliverables this SOW will address].

Delivery phase(s)	***[Insert item and nature of Delivery phase(s), for example, Discovery, Alpha, Beta or Live].***
Overview of Requirement	***[Insert details including Release Types(s), for example, Adhoc, Inception, Calibration or Delivery].***

Accountability Models *Please tick the Accountability Model(s) that shall be used under this Statement of Work:*

Sole Responsibility:☐

Self Directed Team:☐

Rainbow Team:☐

3. BUYER REQUIREMENTS – SOW DELIVERABLES

Outcome Description	Milestone Description Acceptance Criteria
Milestone Ref	

MS01 MS02		
Delivery Plan		
Dependencies		
Supplier Resource Plan		
Security Applicable to SOW:	The Supplier confirms that all Supplier Staff working on Buyer Sites and on Buyer Systems and Deliverables, have completed Supplier Staff Vetting in accordance with Paragraph 6 (Security of Supplier Staff) of Part B – Annex 1 (Baseline Security Requirements) of Call-Off Schedule 9 (Security). [If different security requirements than those set out in Call-Off Schedule 9 (Security) apply under this SOW, these shall be detailed below and apply only to this SOW: *[insert if necessary]*]	

Cyber Essentials Scheme	The Buyer requires the Supplier to have and maintain a Cyber Essentials Plus Certificate for the work undertaken under this SOW, in accordance with Joint Schedule 13 (Cyber Essentials Scheme).
SOW Standards	[Inser any specific Standards applicable to this SOW (check Annex 3 of Framework Schedule 6 (Order Form Template, SOW Template and Call-Off Schedules)]

Performance Management	**[Inser details of Material KPIs that have a material impact on Contract performance]** **Material KPIs Target Measured by** **[Inser Service Levels and/or KPIs – See Call-Off Schedule 14 (Service Levels and Balanced Scorecard)]**
Additional Requirements	**Annex 1 – Where Annex 1 of Joint Schedule 11 (Processing Data) in the Call-Off Contract does not accurately reflect the data Processor / Controller arrangements applicable to this Statement of Work, the Parties shall comply with the revised Annex 1 attached to this Statement of Work.**
Key Supplier Staff	**Key Role Key Staff Contract Details**
Worker Engagement Status	**[Yes / No] [Insert details]**
[SOW Reporting Requirements:]	**[Further to the Supplier providing the management information detailed in Call-Off Schedule 15 (Call-Off Contract Management), the Supplier shall also provide the following additional management information under and applicable to this SOW only:** **Ref. Type of Information Which Services** **1. [insert]** **1.1 [insert] [insert] [insert]]**

4. CHARGES

Call Off Contract Charges	**The applicable charging method(s) for this SOW is:** **[Capped Time and Materials]** **[Incremental Fixed Price]** **[Time and Materials]** **[Fixed Price]** **[2 or more of the above charging methods]** ***[Buyer to select as appropriate for this SOW]*** **The estimated maximum value of this SOW (irrespective of the selected charging method) is £[Insert detail].** **The Charges detailed in the financial model shall be invoiced in accordance with Clause 4 of the Call-Off Contract.**
Rate Cards Applicable	***[Insert SOW applicable Supplier and Subcontractor rate cards from Call-Off Schedule 5 (Pricing Details and Expenses Policy), including details of any discounts that will be applied to the work undertaken under this SOW.]***
Financial Model	***[Supplier to insert its financial model applicable to this SOW]***
Reimbursable Expenses	**[See Expenses Policy in Annex 1 to Call-Off Schedule 5 (Pricing Details and Expenses Policy)]** **[Reimbursable Expenses are capped at [£[Insert] [OR [Insert] percent ([X]%) of the Charges payable under this Statement of Work.]** **[None]** ***[Buyer to delete as appropriate for this SOW]***

5. SIGNATURES AND APPROVALS

Agreement of this SOW

BY SIGNING this Statement of Work, the Parties agree that it shall be incorporated into Appendix 1 of the

For and on behalf of the Supplier	**Name** **and title** **Date** **Signature**
For and on behalf of the Buyer	**Name** **and title** **Date** **Signature**

ANNEX 1 Data Processing

Prior to the execution of this Statement of Work, the Parties shall review Annex 1 of Joint Schedule 11 (Processing Data) and if the contents of Annex 1 does not adequately cover the Processor / Controller arrangements covered by this Statement of Work, Annex 1 shall be amended as set out below and the following table shall apply to the Processing activities undertaken under this Statement of Work only:

Description	Details
Identity of Controller for each Category of Personal Data	**The Relevant Authority is Controller and the Supplier is Processor** **The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:**

Duration of the Processing	**For the duration of this Call Off Contract including any subsequent extensions.** ***]***
Nature and purposes of the Processing **Type of Personal Data**	**Unless otherwise specified pursuant to a SOW,** • **this work involves working on the underlying infrastructure of the new Digital Identity service, including databases within the service, and access logs for the service. The Supplier Personnel pursuant to this Call Off Contract will have access to, and be able to make changes to, the infrastructure containing that information. When the identity proofing aspect of the service is in production there may be sensitive personal data contained within those databases.** **The Supplier Personnel working under this Call Off Contract may have privileged access to data stores, applications, and infrastructure containing sensitive personal information of users.** **The purpose**
Categories of Data Subject	***Users of the Digital Identity service***

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**	

Call Off Special Schedule 1 - Collaboration Agreement

This agreement is made on 7th August 2023.

between:

1) Government Digital Service on behalf of Cabinet Office of The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS (the Buyer)

2) **CAPGEMINI UK PLC,** (company number 00943935) a company incorporated under the laws of England and Wales whose registered office is REDACTED Whereas the:

- Buyer and the Collaboration Suppliers have entered into the Call-Off Contracts (defined below) for the provision of various IT and telecommunications (ICT) services
- Collaboration Suppliers now wish to provide for the ongoing cooperation of the Collaboration Suppliers in the provision of services under their respective Call-Off Contract to the Buyer

In consideration of the mutual covenants contained in the Call-Off Contracts and this Agreement and intending to be legally bound, the parties agree as follows:

1. Definitions and interpretation

1.1 As used in this Agreement, the capitalised expressions will have the following meanings unless the context requires otherwise:

1.1.1 “Agreement” means this collaboration agreement, containing the Clauses and Schedules

1.1.2 “Call-Off Contract” means each contract that is let by the Buyer to one of the Collaboration Suppliers

1.1.3 “Contractor’s Confidential Information” has the meaning set out in the Call-Off Contracts

1.1.4 “Confidential Information” means the Buyer Confidential Information or any Collaboration Supplier's Confidential Information

1.1.5 “Collaboration Activities” means the activities set out in this Agreement

1.1.6 “Buyer Confidential Information” has the meaning set out in the Call-Off Contract

1.1.7 “Default” means any breach of the obligations of any Collaboration Supplier or any Default, act, omission, negligence or statement of any Collaboration Supplier, its employees, servants, agents or subcontractors in connection with or in relation to the subject matter of this Agreement and in respect of which such Collaboration Supplier is liable (by way of indemnity or otherwise) to the other parties

1.1.8 “Detailed Collaboration Plan” has the meaning given in clause 3.2 1.1.9

“Dispute Resolution Process” means the process described in clause 9 1.1.10

“Effective Date” means 7th August 2023

1.1.11 “Force Majeure Event” has the meaning given in clause 11.1.1

1.1.12 “Mediator” has the meaning given to it in clause 9.3.1

1.1.13 “Outline Collaboration Plan” has the meaning given to it in clause 3.1

1.1.14 “Term” has the meaning given to it in clause 2.1

1.1.15 "Working Day" means any day other than a Saturday, Sunday or public holiday in England and Wales

1.2 General

1.2.1 As used in this Agreement the:

1.2.1.1 masculine includes the feminine and the neuter

1.2.1.2 singular includes the plural and the other way round

1.2.1.3 A reference to any statute, enactment, order, regulation or other similar instrument will be viewed as a reference to the statute, enactment, order, regulation or instrument as amended by any subsequent statute, enactment, order, regulation or instrument or as contained in any subsequent re-enactment.

1.2.2 Headings are included in this Agreement for ease of reference only and will not affect the interpretation or construction of this Agreement.

1.2.3 References to Clauses and Schedules are, unless otherwise provided,references to clauses of and schedules to this Agreement.

1.2.4 Except as otherwise expressly provided in this Agreement, all remedies available to any party under this Agreement are cumulative and may be exercised concurrently or separately and the exercise of any one remedy will not exclude the exercise of any other remedy.

1.2.5 The party receiving the benefit of an indemnity under this Agreement will use its reasonable endeavours to mitigate its loss covered by the indemnity.

2. Term of the agreement

2.1 This Agreement will come into force on the Effective Date and, unless earlier terminated in accordance with clause 10, will expire 6 months after the expiry or termination (however arising) of the exit period of the last Call-Off Contract (the "Term").

2.2 A Collaboration Supplier's duty to perform the Collaboration Activities will continue until the end of the exit period of its last relevant Call-Off Contract.

3. Provision of the collaboration plan

3.1 The Collaboration Suppliers will, within 2 weeks (or any longer period as notified by the Buyer in writing) of the Effective Date, provide to the Buyer detailed proposals for the Collaboration Activities they require from each other (the "Outline Collaboration Plan").

3.2 Within 10 Working Days (or any other period as agreed in writing by the Buyer and the Collaboration Suppliers) of the Effective Date, the Buyer will prepare a plan for the Collaboration Activities (the "Detailed Collaboration Plan"). The Detailed Collaboration Plan will include full details of the activities and interfaces that involve all of the Collaboration Suppliers to ensure the receipt of the services under each Collaboration Supplier's respective Call-Off Contract, by the Buyer. The Detailed Collaboration Plan will be based on the Outline Collaboration Plan and will be submitted to the Collaboration Suppliers for approval.

3.3 The Collaboration Suppliers will provide the help the Buyer needs to prepare the Detailed Collaboration Plan.

3.4 The Collaboration Suppliers will, within 10 Working Days of receipt of the Detailed Collaboration Plan, either:

3.4.1 approve the Detailed Collaboration Plan
3.4.2 reject the Detailed Collaboration Plan, giving reasons for the rejection

3.5 The Collaboration Suppliers may reject the Detailed Collaboration Plan under clause 3.4.2 only if it is not consistent with their Outline Collaboration Plan in that it imposes additional, more onerous, obligations on them.

3.6 If the parties fail to agree the Detailed Collaboration Plan under clause 3.4, the dispute will be resolved using the Dispute Resolution Process.

4. Collaboration activities

4.1 The Collaboration Suppliers will perform the Collaboration Activities and all other obligations of this Agreement in accordance with the Detailed Collaboration Plan.

4.2 The Collaboration Suppliers will provide all additional cooperation and assistance as is reasonably required by the Buyer to ensure the continuous delivery of the services under the Call-Off Contract.

4.3 The Collaboration Suppliers will ensure that their respective subcontractors provide all co-operation and assistance as set out in the Detailed Collaboration Plan.

5. Invoicing

5.1 If any sums are due under this Agreement, the Collaboration Supplier responsible for paying the sum will pay within 30 Working Days of receipt of a valid invoice.

5.2 Interest will be payable on any late payments under this Agreement under the Late Payment of Commercial Debts (Interest) Act 1998, as amended.

6. Confidentiality

6.1 Without prejudice to the application of the Official Secrets Acts 1911 to 1989 to any Confidential Information, the Collaboration Suppliers acknowledge that any Confidential Information obtained from or relating to the Crown, its servants or agents is the property of the Crown.

6.2 Each Collaboration Supplier warrants that:

6.2.1 any person employed or engaged by it (in connection with this Agreement in the course of such employment or engagement) will only use Confidential Information for the purposes of this Agreement

6.2.2 any person employed or engaged by it (in connection with this Agreement) will not disclose any Confidential Information to any third party without the prior written consent of the other party

6.2.3 it will take all necessary precautions to ensure that all Confidential Information is treated as confidential and not disclosed (except as agreed) or used other than for the purposes of this Agreement by its employees, servants, agents or subcontractors

6.2.4 neither it nor any person engaged by it, whether as a servant or a consultant or otherwise, will use the Confidential Information for the solicitation of business from the other or from the other party's servants or consultants or otherwise

6.3 The provisions of clauses 6.1 and 6.2 will not apply to any information which is:

6.3.1 or becomes public knowledge other than by breach of this clause 6

6.3.2 in the possession of the receiving party without restriction in relation to disclosure before the date of receipt from the disclosing party

6.3.3 received from a third party who lawfully acquired it and who is under no obligation restricting its disclosure

6.3.4 independently developed without access to the Confidential Information

6.3.5 required to be disclosed by law or by any judicial, arbitral, regulatory or other authority of competent jurisdiction

6.4 The Buyer's right, obligations and liabilities in relation to using and disclosing any Collaboration Supplier's Confidential Information provided under this Agreement and the Collaboration Supplier's right, obligations and liabilities in relation to using and disclosing any of the Buyer's Confidential Information provided under this Agreement, will be as set out in the Call-Off Contract.

7. Warranties

7.1 Each Collaboration Supplier warrant and represent that:

7.1.1 it has full capacity and authority and all necessary consents (including but not limited to, if its processes require, the consent of its parent company) to enter into and to perform this Agreement and that this Agreement is executed by an authorised representative of the Collaboration Supplier

7.1.2 its obligations will be performed by appropriately experienced, qualified and trained personnel with all due skill, care and diligence including but not limited to good industry practice and (without limiting the generality of this clause 7) in accordance with its own established internal processes

7.2 Except as expressly stated in this Agreement, all warranties and conditions, whether express or implied by statute, common law or otherwise (including but not limited to fitness for purpose) are excluded to the extent permitted by law.

8. Limitation of liability

8.1 None of the parties exclude or limit their liability for death or personal injury resulting from negligence, or for any breach of any obligations implied by Section 2 of the Supply of Goods and Services Act 1982.

8.2 Nothing in this Agreement will exclude or limit the liability of any party for fraud or fraudulent misrepresentation.

8.3 Subject always to clauses 8.1 and 8.2, the liability of the Buyer to any Collaboration Suppliers for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of statutory duty or otherwise under this Agreement (excluding Clause 6.4, which will be subject to the limitations of liability set out in the relevant Contract) will be limited to £10 million or 150% of the estimated total contract charges (whichever is greater).

8.4 Subject always to clauses 8.1 and 8.2, the liability of each Collaboration Supplier for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of statutory duty or otherwise under this Agreement will be limited to 150% of the estimated total contract charges.

8.5 Subject always to clauses 8.1, 8.2 and 8.6 and except in respect of liability under clause 6 (excluding clause 6.4, which will be subject to the limitations of liability set out in the Call-Off Contract), in no event will any party be liable to any other for:

8.5.1 indirect loss or damage
8.5.2 special loss or damage
8.5.3 consequential loss or damage
8.5.4 loss of profits (whether direct or indirect)
8.5.5 loss of turnover (whether direct or indirect)
8.5.6 loss of business opportunities (whether direct or indirect)
8.5.7 damage to goodwill (whether direct or indirect)

8.6 Subject always to clauses 8.1 and 8.2, the provisions of clause 8.5 will not be taken as limiting the right of the Buyer to among other things, recover as a direct loss any:

8.6.1 additional operational or administrative costs and expenses arising from a Collaboration Supplier's Default

8.6.2 wasted expenditure or charges rendered unnecessary or incurred by the Buyer arising from a Collaboration Supplier's Default

9. Dispute resolution process

9.1 All disputes between any of the parties arising out of or relating to this Agreement will be referred, by any party involved in the dispute, to the representatives of the parties specified in the Detailed Collaboration Plan.

9.2 If the dispute cannot be resolved by the parties' representatives nominated under clause 9.1 within a maximum of 5 Working Days (or any other time agreed in writing by the parties) after it has been referred to them under clause 9.1, then except if a party seeks urgent injunctive relief, the parties will refer it to mediation under the process set out in clause 9.3 unless the Buyer considers (acting reasonably and considering any objections to mediation raised by the other parties) that the dispute is not suitable for resolution by mediation.

9.3 The process for mediation and consequential provisions for mediation are:

9.3.1 a neutral adviser or mediator will be chosen by agreement between the parties or, if they are unable to agree upon a Mediator within 10 Working Days after a request by one party to the other parties to appoint a Mediator or if the Mediator agreed upon is unable or unwilling to act, any party will within 10 Working Days from the date of the proposal to appoint a Mediator or within 10 Working Days of notice to the parties that he is unable or unwilling to act, apply to the President of the Law Society to appoint a Mediator

9.3.2 the parties will within 10 Working Days of the appointment of the Mediator meet to agree a programme for the exchange of all relevant information and the structure of the negotiations

9.3.3 unless otherwise agreed by the parties in writing, all negotiations connected with the dispute and any settlement agreement relating to it will be conducted in confidence and without prejudice to the rights of the parties in any future proceedings

9.3.4 if the parties reach agreement on the resolution of the dispute, the agreement will be put in writing and will be binding on the parties once it is signed by their authorised representatives

9.3.5 failing agreement, any of the parties may invite the Mediator to provide a non-binding but informative opinion in writing. The opinion will be provided on a without prejudice basis and will not be used in evidence in any proceedings relating to this Agreement without the prior written consent of all the parties

9.3.6 if the parties fail to reach agreement in the structured negotiations within 20 Working Days of the Mediator being appointed, or any longer period the parties agree on, then any dispute or difference between them may be referred to the courts.

9.4 The parties must continue to perform their respective obligations under this Agreement and under their respective Contracts pending the resolution of a dispute.

10. Termination and consequences of termination

10.1 Termination

10.1.1 The Buyer has the right to terminate this Agreement at any time by notice in writing to the Collaboration Suppliers whenever the Buyer has the right to terminate a Collaboration Supplier's Call-Off Contract.

10.1.2 Failure by any of the Collaboration Suppliers to comply with their obligations under this Agreement will constitute a Default under their Call-Off Contract. In this case, the Buyer also has the right to terminate by notice in writing the participation of any Collaboration Supplier to this Agreement and sever its name from the list of Collaboration Suppliers, so that this Agreement will continue to operate between the Buyer and the remaining Collaboration Suppliers.

10.2 Consequences of termination

10.2.1 Subject to any other right or remedy of the parties, the Collaboration Suppliers and the Buyer will continue to comply with their respective obligations under the Call-Off Contracts following the termination (however arising) of this Agreement.

10.2.2 Except as expressly provided in this Agreement, termination of this Agreement will be without prejudice to any accrued rights and obligations under this Agreement.

11. General provisions

11.1 Force majeure

11.1.1 For the purposes of this Agreement, the expression "Force Majeure Event" will mean any cause affecting the performance by a party of its obligations under this Agreement arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control, including acts of God, riots, war or armed conflict, acts of terrorism, acts of government, local government or Regulatory Bodies, fire, flood, storm or earthquake, or disaster but
excluding any industrial dispute relating to any party, the party's personnel or any other failure of a Subcontractor.

11.1.2 Subject to the remaining provisions of this clause 11.1, any party to this Agreement may claim relief from liability for non-performance of its obligations to the extent this is due to a Force Majeure Event.

11.1.3 A party cannot claim relief if the Force Majeure Event or its level of exposure to the event is attributable to its wilful act, neglect or failure to take reasonable precautions against the relevant Force Majeure Event.

11.1.4 The affected party will immediately give the other parties written notice of the Force Majeure Event. The notification will include details of the Force Majeure Event together with evidence of its effect on the obligations of the affected party, and any action the affected party proposes to take to mitigate its effect.

11.1.5 The affected party will notify the other parties in writing as soon as practicable after the Force Majeure Event ceases or no longer causes the affected party to be unable to comply with its obligations under this Agreement. Following the notification, this Agreement will continue to be performed on the terms existing immediately before the Force Majeure Event unless agreed otherwise in writing by the parties.

11.2 Assignment and subcontracting

11.2.1 Subject to clause 11.2.2, the Collaboration Suppliers will not assign, transfer, novate, sub-license or declare a trust in respect of its rights under all or a part of this Agreement or the benefit or advantage without the prior written consent of the Buyer.

11.2.2 Any subcontractors identified in the Detailed Collaboration Plan can perform those elements identified in the Detailed Collaboration Plan to be performed by the Subcontractors.

11.3 Notices

11.3.1 Any notices given under or in relation to this Agreement will be deemed to have been properly delivered if sent by recorded or registered post or by fax and will be deemed for the purposes of this Agreement to have been given or made at the time the letter would, in the ordinary course of post, be delivered or at the time shown on the sender's fax transmission report.

11.3.2 For the purposes of clause 11.3.1, the address of each of the parties are those in the Detailed Collaboration Plan.

11.4 Entire agreement

11.4.1 This Agreement, together with the documents and agreements referred to in it, constitutes the entire agreement and understanding between the parties in

respect of the matters dealt with in it and supersedes any previous agreement between the Parties about this.

11.4.2 Each of the parties agrees that in entering into this Agreement and the documents and agreements referred to in it does not rely on, and will have no remedy in respect of, any statement, representation, warranty or undertaking (whether negligently or innocently made) other than as expressly set out in this Agreement. The only remedy available to each party in respect of any statements, representation, warranty or understanding will be for breach of contract under the terms of this Agreement.

11.4.3 Nothing in this clause 11.4 will exclude any liability for fraud.

11.5 Rights of third parties

Nothing in this Agreement will grant any right or benefit to any person other than the parties or their respective successors in title or assignees, or entitle a third party to enforce any provision and the parties do not intend that any term of this Agreement should be enforceable by a third party by virtue of the Contracts (Rights of Third Parties) Act 1999.

11.6 Severability

If any provision of this Agreement is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, that provision will be severed without effect to the remaining provisions. If a provision of this Agreement that is fundamental to the accomplishment of the purpose of this Agreement is held to any extent to be invalid, the parties will immediately commence good faith negotiations to remedy that invalidity.

11.7 Variations

No purported amendment or variation of this Agreement or any provision of this Agreement will be effective unless it is made in writing by the parties.

11.8 No waiver

The failure to exercise, or delay in exercising, a right, power or remedy provided by this Agreement or by law will not constitute a waiver of that right, power or remedy. If a party waives a breach of any provision of this Agreement this will not operate as a waiver of a subsequent breach of that provision, or as a waiver of a breach of any other provision.

11.9 Governing law and jurisdiction

This Agreement will be governed by and construed in accordance with English law and without prejudice to the Dispute Resolution Process, each party agrees to submit to the exclusive jurisdiction of the courts of England and Wales.

Executed and delivered as an agreement by the parties or their duly authorised attorneys the day and year first above written.

For and on behalf of the Buyer

Signed by:

Full name (capitals): REDACTED
Position: REDACTED
Date:

For and on behalf of the Supplier
Signed by: REDACTED

Full name (capitals): REDACTED
Position: REDACTED
Date:

Collaboration Agreement Schedule 1: List of contracts

Collaboration supplier	Name/reference of contract Effective date of contract

Call Off Special Schedule 2 - SECURITY SCHEDULE FOR DEVELOPMENT

1 Buyer Options

Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements relating to that option set out in the relevant Paragraph:

Buyer risk assessment (see Paragraph 2)		
The Buyer has assessed this Agreement as:	**a higher-risk agreement**	**x**
	a standard agreement	☐
Certifications (see Paragraph 8) (applicable only for standard risk agreements)		
Where the Buyer has assessed this Agreement as a standard risk agreement, the Supplier must have the following Certifications:	**Cyber Essentials Plus**	**x**
	Cyber Essentials	☐
Locations (see Paragraph 1 of the Security Requirements)		
The Supplier and Sub-contractors may store, access or Process Government Data in:	**the United Kingdom only**	**x**
	the United Kingdom and European Economic Area only	☐
	anywhere in the world not prohibited by the Buyer	☐
Support Locations (see Paragraph 1 of the Security Requirements)		
The Supplier and Subcontractors may operate Support Locations in:	**the United Kingdom only**	**x**
	the United Kingdom and European Economic Area only	☐
	anywhere in the world not prohibited by the Buyer	☐

2 Buyer risk assessment

2.1 Where the Buyer has assessed this Agreement as a higher-risk agreement, the Supplier must:

(a) comply with all requirements of this Call-Off Schedule 9 (*Security Management*); and

(b) hold the ISO/IEC 27001:2013 Relevant Certification from a UKAS-approved certification body (see Paragraph 8).

2.2 Where the Buyer has assessed this Agreement as a standard risk agreement, the Supplier must comply with all requirements of this this Call-Off Schedule 9 (*Security Management*) except:

(a) Paragraph 9 (*Security Management Plan*);

(b) paragraph 9 of the Security Requirements (*Code Reviews*);

(c) paragraph 11 of the Security Requirements (*Third-party Software Modules*);

(d) paragraph 12 of the Security Requirements (*Hardware and software support*);

(e) paragraph 13 of the Security Requirements (*Encryption*); and

(f) paragraph 19 of the Security Requirements (*Access Control*).

2.3 Where the Buyer has not made an assessment in the table in Paragraph 1, the Parties must treat this Agreement as a higher-risk agreement.

3 Definitions

3.1 In this Schedule Call-Off Schedule 9 (*Security Management*):

"Anti-virus Software"	**means software that:** **protects the Supplier Information Management System from the possible introduction of Malicious Software;** **scans for and identifies possible Malicious Software in the Supplier Information Management System;** **if Malicious Software is detected in the Supplier Information Management System, so far as possible:** **prevents the harmful effects of the Malicious Software; and** **removes the Malicious Software from the Supplier Information Management System;**
"Breach Action Plan"	**means a plan prepared under paragraph 22.3 of the Security Requirements addressing any Breach of Security;**
"Breach of Security"	**means the occurrence of:** **any unauthorised access to or use of the Services, the Buyer Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement, including the Buyer Data and the Code;** **the loss (physical or otherwise), corruption and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement, including the Buyer Data and the Code; and/or**

	any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements; **the installation of Malicious Software in the:** **Supplier Information Management System;** **Development Environment; or** **Developed System;** **any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the:** **Supplier Information Management System;** **Development Environment; or** **Developed System; and** **includes any attempt to undertake the activities listed in sub-paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:** **was part of a wider effort to access information and communications technology by or on behalf of Central Government Bodies; or** **was undertaken, or directed by, a state other than the United Kingdom**
"Buyer Data"	**means any:** **data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media;** **Personal Data for which the Buyer is a, or the, Data Controller; or** **any meta-data relating to categories of data referred to in paragraphs (a) or (b);** **that is:** **supplied to the Supplier by or on behalf of the Buyer; or** **that the Supplier generates, processes, stores or transmits under this Agreement; and** **for the avoidance of doubt includes the Code and any meta-data relating to the Code.**
"Buyer Data Register"	**means the register of all Buyer Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer, produced and maintained in accordance with paragraph 23 of the Security Requirements;**

"Buyer Equipment"	**means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System;**
"Buyer System"	**means the information and communications technology system used by the Buyer to interface with the Supplier Information Management System or through which the Buyer receives the Services;**
"Certification Default"	**means the occurrence of one or more of the circumstances listed in Paragraph 8.4;**
"Certification Rectification Plan"	**means the plan referred to in Paragraph 8.5(a);**
"Certification Requirements"	**means the requirements set out in paragraph 8.3.**
"CHECK Scheme"	**means the NCSC's scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks**
"CHECK Service Provider"	**means a company which, under the CHECK Scheme:** **has been certified by the National Cyber Security Centre;** **holds "Green Light" status; and** **is authorised to provide the IT Health Check services required by paragraph 18 of the Security Requirements;**
"Code"	**means, in respect of the Developed System:** **the source code;** **the object code;** **third-party components, including third-party coding frameworks and libraries; and** **all supporting documentation.**
"Code Review"	**means a periodic review of the Code by manual or automated means to:** **identify and fix any bugs; and** **ensure the Code complies with:** **the requirements of this Schedule [♦] (*Security Management*); and** **the Secure Development Guidance;**
"Code Review Plan"	**means the document agreed with the Buyer under paragraph 9.3 of the Security Requirements setting out the requirements for, and frequency of, Code Reviews;**
"Code Review Report"	**means a report setting out the findings of a Code Review;**

"Cyber Essentials"	**means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;**
"Cyber Essentials Plus"	**means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;**
"Cyber Essentials Scheme"	**means the Cyber Essentials scheme operated by the National Cyber Security Centre;**
"Developed System"	**means the software or system that the Supplier will develop under this Agreement;**
"Development Activity"	**means any activity relating to the development, deployment maintenance and upgrading of the Developed System, including:** **coding;** **testing;** **code storage; and** **deployment.**
"Development Environment"	**means any information and communications technology system and the Sites that the Supplier or its Sub-contractors will use to provide the Development Activity;**
"EEA"	**means the European Economic Area;**
"End-user Device"	**means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services.**
"Email Service"	**means a service that will send, or can be used to send, emails from the Buyer's email address or otherwise on behalf of the Buyer;**
"HMG Baseline Personnel Security Standard"	**means the employment controls applied to any individual member of the Supplier Personnel that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 6.0, May 2018 (https://assets.publishing.service.gov.uk /government/uploads/system/uploads/attachment_data/file/714002/ HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf), as that document is updated from time to time;**
"IT Health Check"	**means security testing of the Supplier Information Management System, insofar as it relates to the Developed System but excluding the Development Environment in accordance with paragraph 33 of the Security Requirements;**
"Malicious Software"	**means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations;**
"Modules Register"	**means the register of Third-party Software Modules required for higher risk agreements by paragraph 11.3 of the Security Requirements;**

"NCSC"	**means the National Cyber Security Centre;**
"NCSC Cloud Security Principles"	**means the NCSC's document "Implementing the Cloud Security Principles" as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/ implementing-the-cloud-security-principles.**
"NCSC Device Guidance"	**means the NCSC's document "Device Security Guidance", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance;**
"NCSC Protecting Bulk Personal Data Guidance"	**means the NCSC's document "Protecting Bulk Personal Data", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data**
"NCSC Secure Design Principles"	**means the NCSC's document "Secure Design Principles", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cyber-security-design-principles.**
"OWASP"	**means the Open Web Application Security Project Foundation;**
"OWASP Secure Coding Practice"	**means the Secure Coding Practices Quick Reference Guide published by OWASP, as updated or replaced from time to time and found at https://owasp.org/www-project-secure-coding-practices-quick-referen ce-guide/migrated_content;**
"OWASP Top Ten"	**means the list of the most critical security risks to web applications published annually by OWASP and found at https://owasp.org/www-project-top-ten/;**
"Privileged User"	**means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges;**
"Process"	**means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data;**
"Prohibited Activity"	**means the storage, access or Processing of Buyer Data prohibited by a Prohibition Notice;**
"Prohibition Notice"	**means a notice issued under paragraph 1.8 of the Security Requirements.**
"Protective Monitoring System"	**means the system implemented by the Supplier and its Sub-contractors under paragraph 20.1 of the Security Requirements to monitor and analyse access to and use of the Supplier Information Management System, the Development Environment, the Buyer Data and the Code**
"Register of Support Locations and Third-Party Tools"	**means the part of the Security Management Plan setting out, in respect of Support Locations and Third-Party Tools:**

	the nature of the activity performed at the Support Location or by the Third-Party Tool on the Code or the Buyer Data (as applicable); **where that activity is performed by individuals, the place or facility from where that activity is performed; and** **in respect of the entity providing the Support Locations or Third-Party Tools, its:** **full legal name;** **trading name (if any)** **country of registration;** **registration number (if applicable); and** **registered address.**
"Relevant Activities"	**means those activities specified in paragraph 0 of the Security Requirements.**
"Relevant Certifications"	**means** **in the case of a standard agreement:** **Cyber Essentials; and/or** **Cyber Essentials Plus** **as determined by the Buyer; or** **in the case of a higher risk agreement:** **ISO/IEC 27001:2013 by a UKAS-approved certification body in respect of the Supplier Information Management System, or the Supplier Information Management System is included within the scope of a wider certification of compliance with ISO/IEC 27001:2013; and** **Cyber Essentials Plus;**
"Relevant Convictions"	**means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), or any other offences relevant to Services as the Buyer may specify**
"Remediation Action Plan"	**means the plan prepared by the Supplier in accordance with Paragraph 18.11 to 18.15, addressing the vulnerabilities and findings in a IT Health Check report**
"Secure Development Guidance"	**means:** **the NCSC's document "Secure development and deployment guidance" as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/developers-collection; and**

	the OWASP Secure Coding Practice as updated or replaced from time to time;
"Security Management Plan"	**means the document prepared in accordance with the requirements of Paragraph 9 and in the format, and containing the information, specified in Annex 2.**
"SMP Sub-contractor"	**means a Sub-contractor with significant market power, such that:** **they will not contract other than on their own contractual terms; and** **either:** **there are no other substitutable suppliers of the particular services other than SMP Sub-contractors; or** **the Sub-contractor concerned has an effective monopoly on the provision of the Services.**
"Sites"	**means any premises:** **from or at which:** **the Services are (or are to be) provided; or** **the Supplier manages, organises or otherwise directs the provision or the use of the Services; or** **where:** **any part of the Supplier Information Management System is situated; or** **any physical interface with the Buyer System takes place; and** **for the avoidance of doubt include any premises at which Development Activities take place**
"Sub-contractor"	**includes, for the purposes of this Call-Off Schedule 9 (*Security Management*), any individual or entity that:** **forms part of the supply chain of the Supplier; and** **has access to, hosts, or performs any operation on or in respect of the Supplier Information Management System, the Development Environment, the Code and the Buyer Data;**
"Sub-contractor Personnel"	**means:** **any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and** **engaged in or likely to be engaged in:** **the performance or management of the Services;** **or the provision of facilities or services that are necessary for the provision of the Services.**

"Supplier Information Management System"	**means:** **those parts of the information and communications technology system and the Sites that the Supplier or its Sub-contractors will use to provide the Services;** **the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources); and** **for the avoidance of doubt includes the Development Environment.**
"Security Requirements"	**mean the security requirements in Annex 1 to this Call-Off Schedule 9 (*Security Management*)**
"Supplier Personnel"	**means any individual engaged, directly or indirectly, or employed by the Supplier or any Sub-contractor in the management or performance of the Supplier's obligations under this Agreement;**
"Support Location"	**means a place or facility where or from which individuals may access or Process the Code or the Buyer Data;**
"Support Register"	**means the register of all hardware and software used to provide the Services produced and maintained for Higher Risk Agreements in accordance with paragraph 12 of the Security Requirements.**
"Third-party Software Module"	**means any module, library or framework that:** **is not produced by the Supplier or a Sub-contractor as part of the Development Activity; and** **either:** **forms, or will form, part of the Code; or** **is, or will be, accessed by the Developed System during its operation.**
"Third-party Tool"	**means any activity conducted other than by the Supplier during which the Code or the Buyer Data is accessed, analysed or modified or some form of operation is performed on it;**
"UKAS"	**means the United Kingdom Accreditation Service;**

4 Introduction

4.1 This Call-Off Schedule 9 (*Security Management*) sets out:

(a) the assessment of this Agreement as either a:

(i) higher risk agreement; or

(ii) standard agreement,

in Paragraph 1;

(b) the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Agreement to ensure the security of:

(i) the Development Activity;

(ii) the Development Environment;

(iii) the Buyer Data;

(iv) the Services; and

(v) the Supplier Information Management System;

(c) the principle of co-operation between the Supplier and the Buyer on security matters, in Paragraph 5;

(d) the Buyer's access to the Supplier Personnel and Supplier Information Management System, in Paragraph 7;

(e) the Certification Requirements, in Paragraph 8;

(f) the requirements for a Security Management Plan in the case of higher-risk agreements, in Paragraph 9; and

(g) the Security Requirements with which the Supplier and its Sub-contractors must comply.

5 Principles of Security

5.1 The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Buyer Data, and the integrity and availability of the Developed System, and, consequently, on the security of:

(a) the Sites;

(b) the Services; and

(c) the Supplier's Information Management System.

5.2 The Parties shall share information and act in a co-operative manner at all times to further the principles of security in Paragraph 5.1.

5.3 Notwithstanding the involvement of the Buyer in the assurance of the Supplier Information Management System, the Supplier remains responsible for:

(a) the security, confidentiality, integrity and availability of the Buyer Data when that Buyer Data is under the control of the Supplier or any of its Sub-contractors;

(b) the security and integrity of the Developed System; and

(c) the security of the Supplier Information Management System.

5.4 Where the Supplier, a Sub-contractor or any of the Supplier Personnel is granted access to the Buyer System or to the Buyer Equipment, it must comply with and ensure that all such Sub-contractors and Supplier Personnel comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Buyer System or the Buyer Equipment.

6 Security Requirements

6.1 The Supplier shall:

(a) comply with the Security Requirements; and

(b) subject to Paragraph 6.2, ensure that all Sub-contractors also comply with the Security Requirements.

6.2 Where a Sub-contractor is SMP Sub-contractor, the Supplier shall:

(a) use best endeavours to ensure that the SMP Sub-contractor complies with the Security Requirements;

(b) document the differences between Security Requirements the obligations that the SMP Sub-contractor is prepared to accept in sufficient detail to allow the Buyer to form an informed view of the risks concerned;

(c) take such steps as the Buyer may require to mitigate those risks.

7 Access to Supplier Personnel and Supplier Information Management System

7.1 The Buyer may require, and the Supplier must provide, and ensure that each Sub-contractor provides, the Buyer and its authorised representatives with:

(a) access to the Supplier Personnel, including, for the avoidance of doubt, the Sub-contractor Personnel;

(b) access to the Supplier Information Management System, including those parts of the Supplier Information Management System under the control of, or operated by, any Sub-contractor; and

(c) such other information and/or documentation that the Buyer or its authorised representatives may require,

to allow the Buyer to audit the Supplier and its Sub-contractors' compliance with this Call-Off Schedule 9 (*Security Management*) and the Security Requirements.

7.2 The Supplier must provide the access required by the Buyer in accordance with Paragraph 7.1:

(a) in the case of a Breach of Security within 24 hours of such a request; and

(b) in all other cases, within 10 Working Days of such request.

8 Certification Requirements

8.1 The Supplier shall ensure that, unless otherwise agreed by the Buyer, both:

(a) it; and

(b) any Sub-contractor,

is certified as compliant with the Relevant Certifications.

8.2 Unless otherwise agreed by the Buyer, before it begins to provide the Services, the Supplier must provide the Buyer with a copy of:

(a) the Relevant Certifications for it and any Sub-contractor; and

(b) in the case of a higher-risk agreement, any relevant scope and statement of applicability required under the ISO/IEC 27001:2013 Relevant Certifications.

8.3 The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications for it and any Sub-contractor are:

(a) currently in effect;

(b) cover at least the full scope of the Supplier Information Management System; and

(c) are not subject to any condition that may impact the provision of the Services or the Development Activity (the "**Certification Requirements**").

8.4 The Supplier must notify the Buyer promptly, and in any event within three (3) Working Days, after becoming aware that, in respect of it or any Sub-contractor:

(a) a Relevant Certification has been revoked or cancelled by the body that awarded it;

(b) a Relevant Certification expired and has not been renewed by the Supplier;

(c) a Relevant Certification no longer applies to the full scope of the Supplier Information Management System; or

(d) the body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a "**Certification Default**")

8.5 Where the Supplier has notified the Buyer of a Certification Default under Paragraph 8.4:

(a) the Supplier must, within 10 Working Days of the date in which the Supplier provided notice under Paragraph 8.4 (or such other period as the Parties may agree) provide a draft plan (a "**Certification Rectification Plan**") to the Buyer setting out:

(i) full details of the Certification Default, including a root cause analysis;

(ii) the actual and anticipated effects of the Certification Default;

(iii) the steps the Supplier and any Sub-contractor to which the Certification Default relates will take to remedy the Certification Default;

(b) the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;

(c) if the Buyer rejects the Certification Rectification Plan, the Supplier must within 5 Working Days of the date of the rejection submit a revised Certification Rectification Plan and Paragraph (b) will apply to the re-submitted plan;

(d) the rejection by the Buyer of a revised Certification Rectification Plan is a material Default of this Agreement;

(e) if the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

9 Security Management Plan

9.1 This Paragraph 9 applies only where the Buyer has assessed that this Agreement is a higher-risk agreement.

Preparation of Security Management Plan

9.2 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Call-Off Schedule 9 (*Security Management*) and the Agreement in order to ensure the security of the Development Environment, the Developed System, the Buyer Data and the Supplier Information Management System.

9.3 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Agreement, the Security Management Plan, which must include:

(a) an assessment of the Supplier Information Management System against the requirements of this Call-Off Schedule 9 (*Security Management*), including the Security Requirements;

(b) the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Development Environment, the Developed System. the Buyer Data, the Buyer, the Services and/or users of the Services; and

(c) the following information, so far as is applicable, in respect of each Sub-contractor:

(i) the Sub-contractor's:

(A) legal name;

(B) trading name (if any);

(C) registration details (where the Sub-contractor is not an individual);

(ii) the Relevant Certifications held by the Sub-contractor;

(iii) the Sites used by the Sub-contractor;

(iv) the Development Activity undertaken by the Sub-contractor;

(v) the access the Sub-contractor has to the Development Environment;

(vi) the Buyer Data Processed by the Sub-contractor;

(vii) the Processing that the Sub-contractor will undertake in respect of the Buyer Data;

(viii) the measures the Sub-contractor has in place to comply with the requirements of this Call-Off Schedule 9 (*Security Management*);

(d) the Register of Support Locations and Third Party Tools;

(e) the Modules Register;

(f) the Support Register;

(g) details of the steps taken to comply with:

(i) the Secure Development Guidance; and

(ii) the secure development policy required by the ISO/IEC 27001:2013 Relevant Certifications;

(h) details of the protective monitoring that the Supplier will undertake in accordance with paragraph 20 of the Security Requirements, including:

(i) the additional audit and monitoring the Supplier will undertake of the Supplier Information Management System and the Development environment; and

(ii) the retention periods for audit records and event logs.

Approval of Security Management Plan

9.4 The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and must issue the Supplier with either:

(a) an information security approval statement, which shall confirm that the Supplier may use the Supplier Information Management System to:

(i) undertake the Development Activity; and/or

(ii) Process Buyer Data; or

(b) a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.

9.5 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within 10 Working Days of the date of the rejection, or such other period agreed with the Buyer.

9.6 The rejection by the Buyer of a revised Security Management Plan is a material Default of this Agreement.

Updating Security Management Plan

9.7 The Supplier shall regularly review and update the Security Management Plan, and provide such to the Buyer, at least once each year and as required by this Paragraph.

Monitoring

9.8 The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:

(a) a significant change to the components or architecture of the Supplier Information Management System;

(b) a new risk to the components or architecture of the Supplier Information Management System;

(c) a vulnerability to the components or architecture of the Supplier Information Management System using an industry standard vulnerability scoring mechanism;

(d) a change in the threat profile;

(e) a significant change to any risk component;

(f) a significant change in the quantity of Personal Data held within the Service;

(g) a proposal to change any of the Sites from which any part of the Services are provided; and/or

(h) an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

9.9 Within 10 Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Security Management Plan and submit the updated Security Management Plan to the Buyer for review and approval.

Annex 1 Security Requirements

1 Location

Location for Relevant Activities

1.1 Unless otherwise agreed with the Buyer, the Supplier must, and ensure that its Sub-contractors, at all times:

(a) undertake the Development Activity;

(b) host the Development Environment; and

(c) store, access or process Buyer Data,

(the "**Relevant Activities**") only in the geographic areas permitted by the Buyer.

1.2 Where the Buyer has permitted the Supplier and its Sub-contractors to perform the Relevant Activities outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Sub-contractors undertake the Relevant Activities in a facility operated by an entity where:

(a) the entity has entered into a binding agreement with the Supplier or Sub-contractor (as applicable);

(b) that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Sub-contractors in this Schedule 5 (*Security Management*);

(c) the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;

(d) the Supplier has provided the Buyer with such information as the Buyer requires concerning:

(i) the entity;

(ii) the arrangements with the entity; and

(iii) the entity's compliance with the binding agreement; and

(e) the Buyer has not given the Supplier a Prohibition Notice under paragraph 1.8.

1.3 Where the Supplier cannot comply with one or more of the requirements of paragraph 1.2:

(a) it must provide the Buyer with such information as the Buyer requests concerning:

(i) the security controls in places at the relevant location or locations; and

(ii) where certain security controls are not, or only partially, implemented the reasons for this;

(b) the Buyer may grant approval to use that location or those locations, and that approval may include conditions; and

(c) if the Buyer does not grant permission to use that location or those locations, the Supplier must, within such period as the Buyer may specify:

(i) cease to store, access or process Buyer Data at that location or those locations;

(ii) sanitise, in accordance with instructions from the Buyer, such equipment within the information and communications technology system used to store, access or process Buyer Data at that location, or those locations, as the Buyer may specify.

Support Locations

1.4 The Supplier must ensure that all Support Locations are located only in the geographic areas permitted by the Buyer.

1.5 Where the Buyer has permitted the Supplier and its Sub-contractors to operate Support Locations outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Sub-contractors operate the Support Locations in a facility operated by an entity where:

(a) the entity has entered into a binding agreement with the Supplier or Sub-contractor (as applicable);

(b) that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Sub-contractors in this Schedule 5 (*Security Management*);

(c) the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;

(d) the Supplier has provided the Authority with such information as the Authority requires concerning:

(i) the entity;

(ii) the arrangements with the entity; and

(iii) the entity's compliance with the binding agreement; and

(e) the Authority has not given the Supplier notice under paragraph 1.8.

Third-party Tools

1.6 The Supplier must use, and ensure that Sub-contractors use, only those Third-party Tools included in the Register of Support Locations and Third-party Tools.

1.7 The Supplier must not, and must not allow Sub-contractors to, use a new Third-party Tool, or replace an existing Third-party Tool, without the permission of the Buyer.

Prohibited Activities

1.8 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Sub-contractors must not undertake or permit to be undertaken some or all of the Relevant Activities or operate Support Locations (a "**Prohibited Activity**").

(a) in any particular country or group of countries;

(b) in or using facilities operated by any particular entity or group of entities; or

(c) in or using any particular facility or group of facilities, whether operated by the Supplier, a Sub-contractor or a third-party entity,

(a "**Prohibition Notice**").

1.9 Where the Supplier or Sub-contractor, on the date of the Prohibition Notice undertakes any Prohibited Activities affected by the notice, the Supplier must, and must procure that Sub-contractors, cease to undertake that Prohibited Activity within 40 Working Days of the date of the Prohibition Notice.

2 Vetting, Training and Staff Access

Vetting before performing or managing Services

2.1 The Supplier must not engage Supplier Personnel, and must ensure that Sub-contractors do not engage Sub-contractor Personnel in:

(a) Development Activity;

(b) any activity that provides access to the Development Environment; or

(c) any activity relating to the performance and management of the Services

unless:

(d) that individual has passed the security checks listed in paragraph 2.2; or

(e) the Buyer has given prior written permission for a named individual to perform a specific role.

2.2 For the purposes of paragraph 2.1, the security checks are:

(a) the checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:

(i) the individual's identity;

(ii) the individual's nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;

(iii) the individual's previous employment history; and

(iv) that the individual has no Relevant Convictions;

(b) national security vetting clearance to the level specified by the Buyer for such individuals or such roles as the Buyer may specify; or

(c) such other checks for the Supplier Personnel of Sub-contractors as the Buyer may specify.

Annual training

2.3 The Supplier must ensure, and ensure that Sub-contractors ensure, that all Supplier Personnel, complete and pass security training at least once every calendar year that covers:

(a) General training concerning security and data handling; and

(b) Phishing, including the dangers from ransomware and other malware.

Staff access

2.4 The Supplier must ensure, and ensure that Sub-contractors ensure, that individual Supplier Personnel can access only the Buyer Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.

2.5 The Supplier must ensure, and ensure that Sub-contractors ensure, that where individual Supplier Personnel no longer require access to the Buyer Data or any part of the Buyer Data, their access to the Buyer Data or that part of the Buyer Data is revoked immediately when their requirement to access Buyer Data ceases.

2.6 Where requested by the Buyer, the Supplier must remove, and must ensure that Sub-contractors remove, an individual Supplier Personnel's access to the Buyer Data, or part of that Buyer Data specified by the Buyer, as soon as practicable and in any event within 24 hours of the request.

Exception for certain Sub-contractors

2.7 Where the Supplier considers it cannot ensure that a Sub-contractors will undertake the relevant security checks on any Sub-contractor Personnel, it must:

(a) as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;

(b) provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Sub-contractor Personnel will perform as the Buyer reasonably requires; and

(c) comply, at the Supplier's cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Personnel and the management of the Sub-contractor.

3 End-user Devices

3.1 The Supplier must manage, and must ensure that all Sub-contractors manage, all End-user Devices on which Buyer Data or Code is stored or processed in accordance with the following requirements:

(a) the operating system and any applications that store, process or have access to Buyer Data or Code must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;

(b) users must authenticate before gaining access;

(c) all Buyer Data and Code must be encrypted using a encryption tool agreed to by the Buyer;

(d) the End-user Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;

(e) the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Buyer Data and Code to ensure the security of that Buyer Data and Code;

(f) the Suppler or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Buyer Data or Code stored on the device and prevent any user or group of users from accessing the device;

(g) all End-user Devices are within the scope of any Relevant Certification.

3.2 The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Agreement.

3.3 Where there is any conflict between the requirements of this Call-Off Schedule 9 (*Security Management*) and the requirements of the NCSC Device Guidance, the requirements of this Schedule take precedence.

4 Secure Architecture

4.1 The Supplier shall design and build the Developed System in a manner consistent with:

(a) the NCSC's guidance on "Security Design Principles for Digital Services";

(b) where the Developed System will Process bulk data, the NCSC's guidance on "Bulk Data Principles"; and

(c) the NCSC's guidance on "Cloud Security Principles".

4.2 Where any of the documents referred to in paragraph 4.1 provides for various options, the Supplier must document the option it has chosen to implement and its reasons for doing so.

5 Secure Software Development by Design

5.1 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity, implement secure development and deployment practices to ensure that:

(a) no malicious code is introduced into the Developed System or the Supplier Information Management System.

(b) the Developed System can continue to function in accordance with the Specification:

(i) in unforeseen circumstances; and

(ii) notwithstanding any attack on the Developed System using common cyber-attack techniques, including attacks using those vulnerabilities identified at any time in the OWASP Top Ten.

5.2 To those ends, the Supplier must, and ensure that all Sub-contractors engaged in Development Activity:

(a) comply with the Secure Development Guidance as if its requirements were terms of this Contract; and

(b) document the steps taken to comply with that guidance as part of the Security Management Plan.

5.3 In particular, the Supplier must, and ensure that all Sub-contractors engaged in Development Activity:

(a) ensure that all Supplier Staff engaged in Development Activity are:

(i) trained and experienced in secure by design code development;

(ii) provided with regular training in secure software development and deployment;

(b) ensure that all Code:

(i) is subject to a clear, well-organised, logical and documented architecture;

(ii) follows OWASP Secure Coding Practice

(iii) follows recognised secure coding standard, where one is available;

(iv) employs consistent naming conventions;

(v) is coded in a consistent manner and style;

(vi) is clearly and adequately documented to set out the function of each section of code;

(vii) is subject to appropriate levels of review through automated and non-automated methods both as part of:

(A) any original coding; and

(B) at any time the Code is changed;

(c) ensure that all Development Environments:

(i) protect access credentials and secret keys;

(ii) are logically separate from all other environments, including production systems, operated by the Supplier or Sub-contractor;

(iii) require multi-factor authentication to access;

(iv) have onward technical controls to protect the Developed System or the Supplier Information Management System in the event a Development Environment is compromised;

(v) use network architecture controls to constrain access from the Development Environment to the Developed System or the Supplier Information Management System;

6 Code Repository and Deployment Pipeline

7 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity:

7.1 when using a cloud-based code depository for the deployment pipeline, use only a cloud-based code depository that has been assessed against the NCSC Cloud Security Principles;

7.2 ensure user access to code repositories is authenticated using credentials, with passwords or private keys;

7.3 ensure secret credentials are separated from source code.

7.4 run automatic security testing as part of any deployment of the Developed System.

8 Development and Testing Data

8.1 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity, use only anonymised, dummy or synthetic data when using data within the Development Environment for the purposes of development and testing, .

9 Code Reviews

9.1 This paragraph applies where the Buyer has assessed that this Agreement is a higher-risk agreement.

9.2 The Supplier must:

(a) regularly; or

(b) as required by the Buyer

review the Code in accordance with the requirements of this paragraph 9 (a "**Code Review**").

9.3 Before conducting any Code Review, the Supplier must agree with the Buyer:

(a) the modules or elements of the Code subject to the Code Review;

(b) the development state at which the Code Review will take place;

(c) any specific security vulnerabilities the Code Review will assess; and

(d) the frequency of any Code Reviews (the "**Code Review Plan**").

9.4 For the avoidance of doubt, the Code Review Plan may specify different modules or elements of the Code are reviewed at a different development state, for different security vulnerabilities and at different frequencies.

9.5 The Supplier:

(a) must undertake Code Reviews in accordance with the Code Review Plan; and

(b) may undertake Code Reviews by automated means if this is consistent with the approach specified in the Code review Plan.

9.6 No later than 10 Working Days or each Code Review, the Supplier must provide the Buyer with a full, unedited and unredacted copy of the Code Review Report.

9.7 Where the Code Review identifies any security vulnerabilities, the Supplier must:

(a) remedy these at its own cost and expense;

(b) ensure, so far as reasonably practicable, that the identified security vulnerabilities are not present in any other modules or code elements; and

(c) modify its approach to undertaking the Development Activities to ensure, so far as is practicable, the identified security vulnerabilities will not re-occur; and

(d) provide the Buyer with such information as it requests about the steps the Supplier takes under this paragraph 9.7.

10 Third-party Software

10.1 The Supplier must not, and must ensure that Sub-contractors do not, use any software to Process Buyer Data where the licence terms of that software purport to grant the licensor rights to Process the Buyer Data greater than those rights strictly necessary for the use of the software.

11 Third-party Software Modules

11.1 This paragraph 11 applies only where the Buyer has assessed that this Agreement is a higher-risk agreement

11.2 Where the Supplier or a Sub-contractor incorporates a Third-party Software Module into the Code, the Supplier must:

(a) verify the source and integrity of the Third-party Software Module by cryptographic signing or such other measure that provides the same level of assurance;

(b) perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that Third-party Software Module;

(c) continue to monitor any such Third-party Software Module so as to ensure it promptly becomes aware of any newly-discovered security vulnerabilities;

(d) take appropriate steps to minimise the effect of any such security vulnerability on the Developed System.

11.3 The Supplier must produce and maintain a register of all Third-party Software Modules that form part of the Code (the "**Modules Register**").

11.4 The Modules Register must include, in respect of each Third-party Software Module:

(a) full details of the developer of the module;

(b) the due diligence the Supplier undertook on the Third-party Software Module before deciding to use it;

(c) any recognised security vulnerabilities in the Third-party Software Module; and

(d) how the Supplier will minimise the effect of any such security vulnerability on the Developed System.

11.5 The Supplier must:

(a) review and update the Modules Register:

(i) within 10 Working Days of becoming aware of a security vulnerability in any Third-party Software Module; and

(ii) at least once every 6 (six) months;

(b) provide the Buyer with a copy of the Modules Register:

(i) whenever it updates the Modules Register; and

(ii) otherwise when the Buyer requests.

12 Hardware and software support

12.1 This paragraph 12 applies only where the Buyer has assessed that this Agreement is a higher-risk agreement

12.2 The Supplier must ensure that all software used to provide the Services remains at all times in full security support, including any extended or bespoke security support.

12.3 The Supplier must produce and maintain a register of all software that form the Supplier Information Management System (the "**Support Register**").

12.4 The Support Register must include in respect of each item of software:

(a) the date, so far as it is known, that the item will cease to be in mainstream security support; and

(b) the Supplier's plans to upgrade the item before it ceases to be in mainstream security support.

12.5 The Supplier must:

(a) review and update the Support Register:

(i) within 10 Working Days of becoming aware of the date on which, or any change to the date on which, any item of software will cease to be in mainstream security report;

(ii) within 10 Working Days of introducing new software, or removing existing software, from the Supplier Information Management System; and

(iii) at least once every 12 (twelve) months;

(b) provide the Buyer with a copy of the Support Register:

(i) whenever it updates the Support Register; and

(ii) otherwise when the Buyer requests.

12.6 Where any element of the Developed System consists of COTS Software, the Supplier shall ensure:

(a) those elements are always in mainstream or extended security support from the relevant vendor; and

(b) the COTS Software is not more than one version or major release behind the latest version of the software.

12.7 The Supplier shall ensure that all hardware used to provide the Services, whether used by the Supplier or any Sub-contractor is, at all times, remains in mainstream vendor support, that is, that in respect of the hardware, the vendor continues to provide:

(a) regular firmware updates to the hardware; and

(b) a physical repair or replacement service for the hardware.

13 Encryption

13.1 This paragraph applies where the Buyer has assessed that this Agreement is a higher-risk agreement.

13.2 Before Processing any Buyer Data, the Supplier must agree with the Buyer the encryption methods that it and any Sub-contractors that Process Buyer Data will use to comply with this paragraph 13.

13.3 Where this paragraph 13 requires Buyer Data to be encrypted, the Supplier must use, and ensure that Subcontractors use, the methods agreed by the Buyer under paragraph 13.2.

13.4 Notwithstanding anything in the specification for the Developed System or this Agreement, the Supplier must ensure that the Developed System encrypts Buyer Data:

(a) when the Buyer Data is stored at any time when no operation is being performed on it; and

(b) when the buyer Data is transmitted.

13.5 Unless paragraph 13.6 applies, the Supplier must ensure, and must ensure that all Sub-contractors ensure, that Buyer Data is encrypted:

(a) when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and

(b) when transmitted.

13.6 Where the Supplier, or a Sub-contractor, cannot encrypt Buyer Data as required by paragraph 13.5, the Supplier must:

(a) immediately inform the Buyer of the subset or subsets of Buyer Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;

(b) provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption;

(c) provide the Buyer with such information relating to the Buyer Data concerned, the reasons why that Buyer Data cannot be encrypted and the proposed protective measures as the Buyer may require.

13.7 The Buyer, the Supplier and, where the Buyer requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Buyer Data.

13.8 Where the Buyer and Supplier reach agreement, the Supplier must update the Security Management Plan to include:

(a) the subset or subsets of Buyer Data not encrypted and the circumstances in which that will occur;

(b) the protective measure that the Supplier and/or Sub-contractor will put in place in respect of the unencrypted Buyer Data.

13.9 Where the Buyer and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Buyer Data, either party may refer the matter to be determined by an expert in accordance with the Dispute Resolution Procedure.

14 Email

14.1 Notwithstanding anything in the specification for the Developed System or this Agreement, the Supplier must ensure that where the Developed System will provide an Email Service to the Buyer, the Developed System:

(a) supports transport layer security ("**TLS**") version 1.2, or higher, for sending and receiving emails;

(b) supports TLS Reporting ("**TLS-RPT**");

(c) is capable of implementing:

(i) domain-based message authentication, reporting and conformance ("**DMARC**");

(ii) sender policy framework ("**SPF**"); and

(iii) domain keys identified mail ("**DKIM**"); and

(d) is capable of complying in all respects with any guidance concerning email security as issued or updated from time to time by:

(i) the UK Government (current version at https://www.gov.uk/guidance/set-up-government-email-services-securely; or

(ii) the NCSC (current version at https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing).

15 DNS

15.1 Unless otherwise agreed by the Buyer, the Supplier must ensure that the Developed System uses the UK public sector Protective DNS ("**PDNS**") service to resolve internet DNS queries.

16 Malicious Software

16.1 The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier Information Management System.

16.2 The Supplier must ensure that such Anti-virus Software:

(a) prevents the installation of the most common forms of Malicious Software in the Supplier Information Management System and the Development Environment;

(b) is configured to perform automatic software and definition updates;

(c) provides for all updates to be the Anti-virus Software to be deployed within 10 Working Days of the update's release by the vendor;

(d) performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and

(e) where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.

16.3 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Buyer Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

16.4 The Supplier must at all times, during and after the Term, on written demand indemnify the Buyer and keep the Buyer indemnified, against all Losses incurred by, awarded against or agreed to be paid by the Buyer arising from any Breach of Security caused by Malicious Software where the Breach of Security arose from a failure by the Supplier, or a Sub-contractor, to comply with this paragraph .

17 Vulnerabilities

17.1 Unless the Buyer otherwise agrees, the Supplier must ensure that it or any relevant Sub-contractor applies security patches to any vulnerabilities in the Supplier Information Management System no later than:

(a) seven (7) days after the public release of patches for vulnerabilities classified as "critical";

(b) thirty (30) days after the public release of patches for vulnerabilities classified as "important"; and

(c) sixty (60) days after the public release of patches for vulnerabilities classified as "other".

17.2 The Supplier must:

(a) scan the Supplier Information Management System and the Development Environment at least once every month to identify any unpatched vulnerabilities; and

(b) if the scan identifies any unpatched vulnerabilities ensure they are patched in accordance with paragraph 17.1.

17.3 For the purposes of this paragraph 17, the Supplier must implement a method for classifying vulnerabilities to the Supplier Information Management System as “critical”, “important” or “other” that is aligned to recognised vulnerability assessment systems, such as:

(a) the National Vulnerability Database’s vulnerability security ratings; or

(b) Microsoft’s security bulletin severity rating system.

18 Security testing

Responsibility for security testing

18.1 The Supplier is solely responsible for:

(a) the costs of conducting any security testing required by this Paragraph 18 (unless the Buyer gives notice under Paragraph 18.2); and

(b) the costs of implementing any findings, or remedying any vulnerabilities, identified in that security testing.

Security tests by Buyer

18.2 The Supplier may give notice to the Supplier that the Buyer will undertake the security testing required by Paragraph 18.4(a) and 18.4(d).

18.3 Where the Buyer gives notice under Paragraph 18.2:

(a) the Supplier shall provide such reasonable co-operation as the Buyer requests, including:

(i) such access to the Supplier Information Management System as the Buyer may request; and

(ii) such technical and other information relating to the Information Management System as the Buyer requests;

(b) the Buyer must provide a full, unedited and unredacted copy of the report relating to the IT Health Check as soon as reasonably practicable after the Buyer receives a copy of the report; and

(c) for the purposes of Paragraphs 18.8 to 18.17:

(i) the Supplier must treat any IT Health Check commissioned by the Buyer as if it were such a report commissioned by the Supplier; and

(ii) the time limits in Paragraphs 18.8 and 18.11 run from the date on which the Buyer provides the Supplier with the copy of the report under Paragraph (b).

Security tests by Supplier

18.4 The Supplier must:

(a) during the testing of the Developed System and before the Developed System goes live (unless the Buyer gives notice under Paragraph 18.2);

(b) at least once during each Contract Year; and

(c) when required to do so by the Buyer;

undertake the following activities:

(d) conduct security testing of the Supplier Information Management System, insofar as it relates to the Developed System but excluding the Development Environment (an "**IT Health Check**") in accordance with Paragraph 18.5 to 18.7; and

(e) implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph and 18.8 to 18.17.

IT Health Checks

18.5 In arranging an IT Health Check, the Supplier must:

(a) use only a CHECK Service Provider to perform the IT Health Check;

(b) design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier Information Management System and the delivery of the Services.

(c) promptly provide the Buyer with such technical and other information relating to the Information Management System as the Buyer requests;

(d) include within the scope of the IT Health Check such tests as the Buyer requires;

(e) agree with the Buyer the scope, aim and timing of the IT Health Check.

18.6 The Supplier must commission the IT Health Check in accordance with the scope, aim and timing agreed by the Buyer.

18.7 Following completion of an IT Health Check, the Supplier must provide the Buyer with a full, unedited and unredacted copy of the report relating to the IT Health Check without delay and in any event within 10 Working Days of its receipt by the Supplier.

Remedying vulnerabilities

18.8 In addition to complying with Paragraphs 18.4 to 18.17, the Supplier must remedy:

(a) any vulnerabilities classified as critical in the IT Health Check report within 5 Working Days of becoming aware of the vulnerability and its classification;

(b) any vulnerabilities classified as high in the IT Health Check report within 1 month of becoming aware of the vulnerability and its classification; and

(c) any vulnerabilities classified as medium in the IT Health Check report within 3 months of becoming aware of the vulnerability and its classification.

18.9 The Supplier must notify the Buyer immediately if it does not, or considers it will not be able to, remedy the vulnerabilities classified as critical, high or medium in the IT Health Check report within the time periods specified in Paragraph 18.8.

Significant vulnerabilities

18.10 Where the IT Health Check report identifies more than 10 vulnerabilities classified as either critical or high, the Buyer may, at the Supplier's cost, appoint an independent and appropriately qualified and

experienced security architect and adviser to perform a root cause analysis of the identified vulnerabilities.

Responding to an IT Health Check report

18.11 Where the IT Health Check identifies vulnerabilities in, or makes findings in respect of, the Information Management System, the Supplier must within 20 Working Days of receiving the IT Health Check report, prepare and submit for approval to the Buyer a draft plan addressing the vulnerabilities and findings (the "**Remediation Action Plan**").

18.12 Where the Buyer has commissioned a root cause analysis under Paragraph 18.10, the Supplier shall ensure that the draft Remediation Action Plan addresses that analysis.

18.13 The draft Remediation Action Plan must, in respect of each vulnerability identified or finding made by the IT Health Check report:

(a) how the vulnerability or finding will be remedied;

(b) the date by which the vulnerability or finding will be remedied; and

(c) the tests that the Supplier proposes to perform to confirm that the vulnerability has been remedied or the finding addressed.

18.14 The Supplier shall promptly provide the Buyer with such technical and other information relating to the Supplier Information Management System, the IT Health Check report or the draft Remediation Action Plan as the Buyer requests.

18.15 The Buyer may:

(a) reject the draft Remediation Action Plan where it considers that the draft Remediation Action Plan is inadequate, providing its reasons for doing so, in which case:

(i) the Supplier shall within 10 Working Days of the date on which the Buyer rejected the draft Remediation Action Plan submit a revised draft Remediation Action Plan that takes into account the Buyer's reasons; and

(ii) paragraph 18.13 to 18.15 shall apply, with appropriate modifications, to the revised draft Remediation Action Plan;

(b) accept the draft Remediation Action Plan, in which case the Supplier must immediately start work on implementing the Remediation Action Plan in accordance with Paragraph 18.16 and 18.17.

Implementing an approved Remediation Action Plan

18.16 In implementing the Remediation Action plan, the Supplier must conduct such further tests on the Supplier Information Management System as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has fully and correctly implemented.

18.17 If any such testing identifies a new risk, new threat, vulnerability or exploitation technique with the potential to affect the security of the Supplier Information Management System, the Supplier shall within [2] Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique:

(a) provide the Buyer with a full, unedited and unredacted copy of the test report;

(b) implement interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available;

(c) as far as practicable, remove or disable any extraneous interfaces, services or capabilities not needed for the provision of the Services within the timescales set out in the test report or such other timescales as may be agreed with the Buyer.

19 Access Control

19.1 This paragraph applies where the Buyer has assessed that this Agreement is a higher-risk agreement.

19.2 The Supplier must, and must ensure that all Sub-contractors:

(a) identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;

(b) require multi-factor authentication for all user accounts that have access to Buyer Data or that are Privileged Users;

(c) allow access only to those parts of the Supplier Information Management System and Sites that those persons require;

(d) maintain records detailing each person's access to the Supplier Information Management System and Sites, and make those records available to the Buyer on request.

19.3 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that the user accounts for Privileged Users of the Supplier Information Management System:

(a) are allocated to a single, individual user;

(b) are accessible only from dedicated End-user Devices;

(c) are configured so that those accounts can only be used for system administration tasks;

(d) require passwords with high complexity that are changed regularly;

(e) automatically log the user out of the Supplier Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive; and

(f) in the case of a higher-risk agreement are:

(i) restricted to a single role or small number of roles;

(ii) time limited; and

(iii) restrict the Privileged User's access to the internet.

19.4 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that it logs all activity of the Privileged Users while those users access those accounts and keeps the activity logs for 20 Working Days before deletion.

19.5 The Supplier must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different high-complexity passwords for their different accounts on the Supplier Information Management System.

19.6 The Supplier must ensure that the Developed System is developed and configured so as to provide for the matters set out in paragraphs 19.2 to 19.5.

19.7 The Supplier must, and must ensure that all Sub-contractors:

(a) configure any hardware that forms part of the Supplier Information Management System that is capable of requiring a password before it is accessed to require a password; and

(b) change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.

20 Event logging and protective monitoring

Protective Monitoring System

20.1 The Supplier must, and must ensure that Sub-contractors, implement an effective system of monitoring and reports analysing access to and use of the Supplier Information Management System, the Development Environment, the Buyer Data and the Code to:

(a) identify and prevent potential Breaches of Security;

(b) respond effectively and in a timely manner to Breaches of Security that do occur;

(c) identify and implement changes to the Supplier Information Management System to prevent future Breaches of Security; and

(d) help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier Information Management System or the Developed System

(the "**Protective Monitoring System**").

20.2 The Protective Monitoring System must provide for:

(a) event logs and audit records of access to the Supplier Information Management system; and

(b) regular reports and alerts to identify:

(i) changing access trends;

(ii) unusual usage patterns; or

(iii) the access of greater than usual volumes of Buyer Data;

(c) the detection and prevention of any attack on the Supplier Information Management System or the Development Environment using common cyber-attack techniques;

(d) any other matters required by the Security Management Plan.

Event logs

20.3 The Supplier must ensure that, unless the Buyer otherwise agrees, any event logs do not log:

(a) personal data, other than identifiers relating to users; or

(b) sensitive data, such as credentials or security keys.

Provision of information to Buyer

20.4 The Supplier must provide the Buyer on request with:

(a) full details of the Protective Monitoring System it has implemented; and

(b) copies of monitoring logs and reports prepared as part of the Protective Monitoring System.

Changes to Protective Monitoring System

20.5 The Buyer may at any time require the Supplier to update the Protective Monitoring System to:

(a) respond to a specific threat identified by the Buyer;

(b) implement additional audit and monitoring requirements; and

(c) stream any specified event logs to the Buyer's security information and event management system.

21 Audit rights

Right of audit

21.1 The Buyer may undertake an audit of the Supplier or any Sub-contractor to:

(a) verify the Supplier's or Sub-contractor's (as applicable) compliance with the requirements of this Call-Off Schedule 9 (*Security Management*) and the Data Protection Laws as they apply to Buyer Data;

(b) inspect the Supplier Information Management System (or any part of it);

(c) review the integrity, confidentiality and security of the Buyer Data; and/or

(d) review the integrity and security of the Code.

21.2 Any audit undertaken under this Paragraph 21:

(a) may only take place during the Term and for a period of 18 months afterwards; and

(b) is in addition to any other rights of audit the Buyer has under this Agreement.

21.3 The Buyer may not undertake more than one audit under Paragraph 21.1 in each calendar year unless the Buyer has reasonable grounds for believing:

(a) the Supplier or any Sub-contractor has not complied with its obligations under this Agreement or the Data Protection Laws as they apply to the Buyer Data;

(b) there has been or is likely to be a Security Breach affecting the Buyer Data or the Code; or

(c) where vulnerabilities, or potential vulnerabilities, in the Code have been identified by:

(i) an IT Health Check; or

(ii) a Breach of Security.

Conduct of audits

21.4 The Authority must use reasonable endeavours to provide 15 Working Days' notice of an audit.

21.5 The Authority must when conducting an audit:

(a) comply with all relevant policies and guidelines of the Supplier or Sub-contractor (as applicable) concerning access to the Supplier Information Management System the Buyer considers reasonable having regard to the purpose of the audit; and

(b) use reasonable endeavours to ensure that the conduct of the audit does not unreasonably disrupt the Supplier or Sub-contractor (as applicable) or delay the provision of the Services.

21.6 The Supplier must, and must ensure that Sub-contractors, on demand provide the Buyer with all co-operation and assistance the Buyer may reasonably require, including:

(a) all information requested by the Buyer within the scope of the audit;

(b) access to the Supplier Information Management System; and

(c) access to the Supplier Staff.

Response to audit findings

21.7 Where an audit finds that:

(a) the Supplier or a Sub-contractor has not complied with this Agreement or the Data Protection Laws as they apply to the Buyer Data; or

(b) there has been or is likely to be a Security Breach affecting the Buyer Data

the Buyer may require the Supplier to remedy those defaults at its own cost and expense and within the time reasonably specified by the Buyer.

21.8 The exercise by the Buyer of any rights it may have under this Paragraph 3 does not affect the exercise by it of any other or equivalent rights it may have under this Agreement in respect of the audit findings.

22 Breach of Security

Reporting Breach of Security

22.1 If either party becomes aware of a Breach of Security it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within 24 hours.

Immediate steps

22.2 The Supplier must, upon becoming aware of a Breach of Security immediately take those steps identified in the Security Management Plan (if applicable) and all other steps reasonably necessary to:

(a) minimise the extent of actual or potential harm caused by such Breach of Security;

(b) remedy such Breach of Security to the extent possible;

(c) apply a tested mitigation against any such Breach of Security; and

(d) prevent a further Breach of Security in the future which exploits the same root cause failure;

Subsequent action

22.3 As soon as reasonably practicable and, in any event, within 5 Working Days, or such other period agreed with the Buyer, following the Breach of Security, provide to the Buyer:

(a) full details of the Breach of Security; and

(b) if required by the Buyer:

(i) a root cause analysis; and

(ii) a draft plan addressing the root cause of the Breach of Security

(the "**Breach Action Plan**").

22.4 The draft Breach Action Plan must, in respect of each issue identified in the root cause analysis:

(a) how the issue will be remedied;

(b) the date by which the issue will be remedied; and

(c) the tests that the Supplier proposes to perform to confirm that the issue has been remedied or the finding addressed.

22.5 The Supplier shall promptly provide the Buyer with such technical and other information relating to the draft Breach Action Plan as the Buyer requests.

22.6 The Buyer may:

(a) reject the draft Breach Action Plan where it considers that the draft Breach Action Plan is inadequate, providing its reasons for doing so, in which case:

(i) the Supplier shall within 10 Working Days of the date on which the Buyer rejected the draft Breach Action Plan submit a revised draft Breach Action Plan that takes into account the Buyer's reasons; and

(ii) paragraph 22.5 and 22.6 shall apply to the revised draft Breach Action Plan;

(b) accept the draft Breach Action Plan, in which case the Supplier must immediately start work on implementing the Breach Action Plan.

Assistance to Buyer

22.7 Where the Breach of Security concerns or is connected with the Buyer Data or the Code, the Supplier must provide such assistance to the Buyer as the Buyer requires until the Breach of Security and any impacts or potential impacts on the Buyer are resolved to the Buyer's satisfaction.

22.8 The obligation to provide assistance under Paragraph 22.7 continues notwithstanding the expiry or termination of this Contract.

Reporting of Breach of Security to regulator

22.9 Where the Law requires the Supplier report a Breach of Security to the appropriate regulator, the Supplier must:

(a) make that report within the time limits:

(i) specified by the relevant regulator; or

(ii) otherwise required by Law;

(b) to the extent that the relevant regulator or the Law permits, provide the Buyer with a full, unredacted and unedited copy of that report at the same time it is sent to the relevant regulator.

22.10 Where the Law requires the Buyer to report a Breach of Security to the appropriate regulator, the Supplier must:

(a) provide such information and other input as the Buyer requires within the timescales specified by the Buyer;

(b) where Paragraph 7 applies to the Breach of Security, ensure so far as practicable the report it sends to the relevant regulator is consistent with the report provided by the Buyer.

23 Return and Deletion of Buyer Data

23.1 The Supplier must create and maintain a register of:

(a) all Buyer Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer; and

(b) those parts of the Supplier Information Management System, including those parts of the Supplier Information Management System that are operated or controlled by any Sub-contractor, on which the Buyer Data is stored (the "**Buyer Data Register**").

23.2 The Supplier must:

(a) review and update the Buyer Data Register:

(i) within 10 Working Days of the Supplier or any Sub-contractor changes to those parts of the Supplier Information Management System on which the Buyer Data is stored;

(ii) within 10 Working Days of a significant change in the volume, nature or overall sensitivity of the Buyer Data stored on the Supplier Information Management System;

(iii) at least once every 12 (twelve) months; and

(b) provide the Buyer with a copy of the Buyer Data Register:

(i) whenever it updates the Buyer Data Register; and

(ii) otherwise when the Buyer requests.

23.3 The Supplier must, and must ensure that all Sub-contractors, securely erase any or all Buyer Data held by the Supplier or Sub-contractor, including any or all Code:

(a) when requested to do so by the Buyer; and

(b) using a deletion method agreed with the Buyer that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.

23.4 The Supplier must, and must ensure that all Sub-contractors, provide the Buyer with copies of any or all Buyer Data held by the Supplier or Sub-contractor, including any or all Code:

(a) when requested to do so by the Buyer; and

(b) using the method specified by the Buyer.

Security Management Plan

WP2153 - DevOps Support

Government Digital Service on behalf of Cabinet Office and Capgemini UK plc

Dated: 2023

Owner:

Contents

- **Note - Where any of the responses towards these Template questions have been provided previously, indicate within the question that 'such information has already been issued to Buyer'.**

1 Executive summary

[*This section should contain a brief summary of the business context of the system, the assurance work done, any off-shoring considerations and any significant residual risks that need acceptance.*]

1.1 Change history

Version Number	Date of Change	Change made by	Nature and reason for change

1.2 References, links and dependencies

ID	Document Title	Reference	Date

1.3 Supplier personnel

Key Personnel Names	Title	Contact Details incl. Mobile Number and Email Address

2 System description

2.1 Background

[*A short description of the project/product/system. Describe its purpose, functionality, aim and scope.*]

2.2 Organisational Ownership/Structure

[*Who owns the system and operates the system and the organisational governance structure. This should include how any ongoing security management is integrated into the project governance e.g. how a Security Working Group reports to the project group.*]

2.3 Information assets and flows

(a) Logical data flow diagram

[*This should include a simple high level logical diagram on one page. The diagram must include any third party suppliers and the data flows to/from them.*]

(b) Data assets

[*Include a table of the type and volumes of data that will be Processed, managed and stored within the supplier system. If personal data, please include the fields used such as name, address, department DOB, NI number etc. Data Processed by third party suppliers must be included here*]

2.4 System architecture

[A description of the physical system architecture, to include the system management. Please provide a diagram.]

2.5 Users

[*Please provide a table of the system users, this should include all users including HMG users as well as any service provider users and system managers. If relevant, security clearance level requirements should be included.*]

2.6 Locations

[Please provide a table of where the Authorities data assets are stored, Processed and any locations they are managed from. This must include the locations of any help desks or call centres if relevant. All third party suppliers and subcontractors must be included in this section. Any off-shoring considerations should be detailed with the legal basis for the data transfer included e.g. International Data Transfer Agreements/IDTA's - Transfer Risk Assessments, equivalency etc.]

2.7 Certifications

[*Please include a table of any independent security certifications (e.g. ISO 27001:2013, Cyber Essentials Plus and Cyber Essentials) held as required by the contract. The table should include any relevant third party suppliers or subcontractors and must include the expiry date of the certification. Copies of the certificates should be included in Appendix 1.*]

2.8 Test and development systems

[*Include information about any test, development and User Acceptance testing systems, their locations and whether they contain live system data.*]

3 Risk assessment

3.1 Accreditation/assurance scope

[*This section should describe the scope of the Risk Assessment and should indicate the components of the architecture upon which reliance is placed but assurance will not be done e.g. a cloud hosting service or a SAAS product/tool. A logical diagram should be used along with a brief description of the components. This scope must be agreed by the Authority.*]

3.2 Risk appetite

[*A risk appetite should be provided by the Authority and included here.*]

3.3 Business impact assessment

[*A description of the information assets and the impact of their loss or corruption (e.g. large amounts of Official Sensitive personal data the loss of which would be severely damaging to individuals, embarrassing to HMG, and make HMG liable to ICO investigations) in business terms should be included. This section should cover the impact on loss of confidentiality, integrity and availability of the assets and should be agreed with the Authority. The format of this assessment may be dependent on the risk assessment method chosen.*]

3.4 Risk assessment

[*The content of this section will depend on the risk assessment methodology chosen, but should contain the output of the formal information risk assessment in a prioritised list using business language. Experts on the system and business process should have been involved in the risk assessment to ensure the formal risk methodology used has not missed out any risks. The example table below should be used as the format to identify the risks and document the controls used to mitigate those risks.*]

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level

3.5 Controls

[*The controls listed above to mitigate the risks identified should be detailed. There should be a description of each control, further information and configuration details where relevant, and an assessment of the implementation status of, and assurance in, the control. A sample layout is included below.*]

ID	Control title	Control description	Further information and assurance status

3.6 Residual risks and actions

[*A summary of the residual risks which are likely to be above the risk appetite stated after all controls have been applied and verified should be listed with actions and timescales included.*]

4 In-service controls

[*This section should describe how the main Security Requirements as specified in the contract (security schedule) are met.*]

4.1 Protective monitoring

[*This section should describe how your protective monitoring arrangements identify anomalous behaviour and how this is then acted upon as well as how logging and auditing of user activity is done.*]

4.2 Malware prevention

[*This should describe how your anti-virus solution is implemented with respect to protecting Authority assets.*]

4.3 End user devices

[*This section should detail the security controls which are implemented on all fixed and removable end user devices used to Process, store or manage Authority data.*]

4.4 Encryption

[*This section should detail the encryption measures you employ to protect Authority data both in transit and at rest.*]

4.5 Vulnerability management

[*This section should detail your process for identifying, classifying, prioritising, remediating, and mitigating" software vulnerabilities within your IT environment.*]

4.6 Identity, verification and access controls

[*This section should detail your password policy, your approach to ensuring that privileged accounts are accessible only from end-user devices dedicated to that use and by authenticated named users. This should include your use of multi-factor authentication for all accounts that have access to Authority data as well as privileged accounts.*]

4.7 Data Deletion

[*This section should include the agreed process for securely deleting Authority data when required.*]

5 Supply chain security and third party subcontractors/tools

[*This section should detail the assurance process for managing any security risks from Subcontractors and Third Parties authorised by the Authority with access to Authority data.*]

6 Security Requirements on participating departments, customers and users

[*Please detail any Security Requirements or codes of connection required by participating departments/agencies/third parties.*]

7 Personnel security

[*Please provide details of your Personnel Security Vetting Policy for those staff who will have access to, or come into contact with Buyer data or assets. Outline the employment pre-employment/qualification checks within your organisation.*

Please provide details of how you will ensure that all staff accessing Buyer data are aware of the confidential nature of the data and comply with their legal and specific obligations under the Contract?]

8 Business continuity

[*Please provide an overview of your organisation's business continuity and disaster recovery plans in terms of the Buyer data under the Contract, or attach a copy of your Business Continuity Plan.*]

9 Physical security

[*Please provide details of the building where the service will operate from and describe the procedures and security in place to control access to premises and any areas holding Buyer assets. Detail measures such as construction of buildings used for handling Buyer assets, availability of lockable storage, procedures covering end of day/silent hours, key management, visitor controls.*

Please also include details of any automated access controls, alarms and CCTV coverage. Please also provide details of the maintenance schedule of these security controls.> For the locations where Authority assets are held please provide details of any procedures and security in place designed to control access to the site perimeter. Please detail the measures in place such as fencing, CCTV, guarding, and procedures and controls to handle staff and visitors requesting access to the site. Please also provide details of the maintenance schedule of your security controls.]

10 Major hardware and software and end of support dates

[*This should be a table which lists the end of support dates for hardware and software products and components. An example table is shown below.*]

Name	Version	End of mainstream Support/Extended Support	Notes/RAG Status

11 Incident management process

[*The suppliers' process, as agreed with the Authority/Customer, should be included here. It must as a minimum include the protocol for how and when incidents will be reported to the Authority/customer and the process that will be undertaken to mitigate the incidents and investigate the root cause.*]

12 Required Changes Register

[*The table below shows the headings for the Required Changes Register which should be maintained and used to update the contents of this document at least annually.*]

Ref	Section	Change	Agreed With	Date agreed	Documentation update	Status

Appendix 1 ISO27001/ISO27701 and/or Cyber Essentials Plus certificates

[*Please include copies of the certificates here*]

Appendix 2 Cloud security principles assessment

[*Please add your controls in the attached table.*]

Principle	Goals of the Principle	Controls
Principle 1 – Data in transit protection **"User data transiting networks should be adequately protected against tampering and eavesdropping."**	**• Data in transit is protected between end user device(s) and the service** **• Data in transit is protected internally within the service** **• Data in transit is protected between the service and other services (e.g. where APIs are exposed)**	
Principle 2 – Asset protection and resilience **"User data, and the assets storing or Processing it, should be protected against physical tampering, loss, damage or seizure."**	**Cloud service consumers should seek to understand:** **• In which countries their data will be stored, Processed and managed. They should also consider how this affects compliance with relevant legislation e.g. Data Protection Act (DPA), GDPR etc.** **• Whether the legal jurisdiction(s) within which the service provider operates are acceptable to them**	
Principle 3 – Separation between users **"A malicious or compromised user of the service should not be able to affect the service or data of another."**	**Cloud service consumers should seek to:** **• Understand the types of user they share the service or platform with** **• Have confidence that the service provides sufficient separation of their data and service from other users of the service** **• Have confidence that management of their service is kept separate from other users (covered separately as part of Principle 9)**	

Principle	Goals of the Principle	Controls
Principle 4 – Governance framework **"The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined."**	**Cloud service consumers should ensure that:** **• A clearly identified, and named, board representative (or a person with the direct delegated authority) is responsible for the security of the cloud service. This is typically someone with the title 'Chief Security Officer', 'Chief Information Officer' or 'Chief Technical Officer'** **• A documented framework exists for security governance, with policies governing key aspects of information security relevant to the service** **• Security and information security are part of the service provider's financial and operational risk reporting mechanisms, ensuring that the service provider's board would be kept informed of security and information risk** **• Processes to identify and ensure compliance with applicable legal and regulatory requirements have been established**	
Principle 5 – Operational security **"The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes."**	**Cloud service consumers should be confident that:** **• The status, location and configuration of service components (both hardware and software) are tracked throughout their lifetime** **• Changes to the service are assessed for potential security impact. Then managed and tracked through to completion**	
Principle 6 – Personnel security	**Cloud service consumers should be confident that:**	

Principle	Goals of the Principle	Controls
"Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel."	**• The level of security screening conducted on service provider staff with access to the consumers information, or with ability to affect the service, is appropriate** **• The minimum number of people necessary have access to the consumers information or could affect the service**	
Principle 7 – Secure development **"Services should be designed and developed to identify and mitigate threats to their security.** **Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity."**	**Cloud service consumers should be confident that:** **• New and evolving threats are reviewed, and the service improved in line with them** **• Development is carried out in line with industry good practice regarding secure design, coding, testing and deployment** **• Configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment**	
Principle 8 – Supply chain security **"The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement."**	**Cloud service consumers should seek to understand and accept:** **• How their information is shared with, or accessible to, third party suppliers and their supply chains** **• How the service provider's procurement processes place security requirements on third party suppliers** **• How the service provider manages security risks from third party suppliers** **• How the service provider manages the conformance of their suppliers with security requirements**	

Principle	Goals of the Principle	Controls
	• How the service provider verifies that hardware and software used in the service is genuine and has not been tampered with	
Principle 9 – Secure user management "Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data."	Cloud service consumers should: • Be aware of all of the mechanisms by which the service provider would accept management or support requests from you (telephone, web portal, email etc.) • Ensure that only authorised individuals from their organisation can use those mechanisms to affect their use of the service (Principle 10 can help consumers consider the strength of user identification and authentication in each of these mechanisms)	
Principle 10 – Identity and authentication "All access to service interfaces should be constrained to authenticated and authorised individuals."	Cloud service consumers should: • Have confidence that identity and authentication controls ensure users are authorised to access specific interfaces	
Principle 11 – External interface protection "All external or less trusted interfaces of the service should be identified and appropriately defended."	Cloud service consumers should: • Understand what physical and logical interfaces their information is available from, and how access to their data is controlled • Have sufficient confidence that the service identifies and authenticates users to an appropriate level over those interfaces (see Principle 10)	

Principle	Goals of the Principle	Controls
Principle 12 – Secure service administration **"Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data."**	**Cloud service consumers should:** **• Understand which service administration model is being used by the service provider to manage the service** **• Be content with any risks the service administration model in use brings to the consumers data or use of the service**	
Principle 13 – Audit information for users **"You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales."**	**Cloud service consumers should:** **• Be aware of the audit information that will be provided, how and when it will be made available, the format of the data, and the retention period associated with it** **• Be confident that the audit information available will meet their needs for investigating misuse or incidents**	
Principle 14 – Secure use of the service **"The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected."**	**Cloud service consumers should:** **• Understand any service configuration options available to them and the security implications of their choices** **• Understand the security requirements of their use of the service** **• Educate their staff using and managing the service in how to do so safely and securely**	

Appendix 3 Protecting bulk data assessment if required by the authority/customer

[*A spreadsheet may be attached*]

Appendix 4 Latest ITHC report and vulnerability correction plan

Appendix 5 Statement of applicability

[This should be a completed ISO 27001:2013 Statement of Applicability for the Information Management System if ISO27001 certification is required by the Contract.]