Cabinet Office

Digital Outcomes and Specialists 5 (RM1043.7)

Version 2

Provision of Online Tooling Platform - Private & Public Beta

CONTRACT REFERENCE: C2328

CONTRACT FOR

CENTRAL DIGITAL & DATA OFFICE (CDDO)

CABINET OFFICE

FEBRUARY 2023

Cabinet Office

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

1. Order Form

Call-Off Reference: C2328

Call-Off Title: Provision of Performance & Assurance Online Tooling Platform

Call-Off Contract Description: To build an Online Tooling Platform to support spending and commercial controls.

The Buyer: Cabinet Office Central Digital & Data Office

Buyer Address: **REDACTED TEXT under FOIA Section 40, Personal Information**

The Supplier: Rainmaker Solutions Ltd

Supplier Address: **REDACTED TEXT under FOIA Section 40, Personal Information**

Registration Number: 07408622

DUNS Number: 216944423

2. Applicable Framework Contract

This Order Form is for the provision of the Call-Off Deliverables and dated 8th March 2023.

- It is issued under the Framework Contract with the reference number RM1043.7 for the provision of Digital Outcomes and Specialists Deliverables.
- The Parties intend that this Call-Off Contract will not, except for the first Statement of Work which shall be executed at the same time that the Call-Off Contract is executed, 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, Statement of Work 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.

3. Call-Off Lot

Lot 1 Digital Outcomes

4. 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) RM1043.7

3 Framework Special Terms

4 The following Schedules in equal order of precedence:

- Joint Schedules for RM1043.7
    - Joint Schedule 2 (Variation Form)
    - Joint Schedule 3 (Insurance Requirements)
    - Joint Schedule 4 (Commercially Sensitive Information)
    - Joint Schedule 5 (Corporate Social Responsibility) RM1043.7
    - Joint Schedule 6 (Key Subcontractors)
    - Joint Schedule 10 (Rectification Plan)
    - Joint Schedule 11 (Processing Data) RM1043.7
    - Joint Schedule 12 (Supply Chain Visibility)
- Call-Off Schedules for RM1043.7
    - Call-Off Schedule 1 (Transparency Reports)
    - Call-Off Schedule 3 (Continuous Improvement)
    - Call-Off Schedule 5 (Pricing Details and Expenses Policy)
    - Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables)
    - Call-Off Schedule 7 (Key Supplier Staff)
    - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
    - Call-Off Schedule 9 (Security)
    - Call-Off Schedule 10 (Exit Management)
    - Call-Off Schedule 13 (Implementation Plan and Testing)
    - Call-Off Schedule 14 (Service Levels and Balanced Scorecard)
    - Call-Off Schedule 15 (Call-Off Contract Management)
    - Call-Off Schedule 20 (Call-Off Specification)
    - Call-Off Schedule 26 (Cyber Essentials Scheme)

5 CCS Core Terms (version 3.0.9)

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.

5. Call-Off Special Terms-

The following Special Terms are incorporated into this Call-Off Contract:

1. Call-Off Start Date: 8th March 2023
2. Call-Off Expiry Date: 7th March 2024
3. Call-Off Optional Extension Period: 1 year
4. Minimum Notice Period for Extensions: 4 weeks
5. Call-Off Contract Value: £813,950.00 (Ex VAT)
6. Buyer's Digital and Technology Special Terms
    a. No special terms
7. Buyer's Information Assurance Special Terms

a. The Supplier must hold a current Cyber Essentials Plus certificate for the entire term of the contract, with a scope appropriate to the networks and end-user devices used to process CDDO owned data or connect to CDDO's productivity suites.
b. The supplier must adhere to the security requirements outlined in Call-Off Schedule 9 Annex 1 contained in Call-Off Schedules for The Provision of Online Tooling Platform - Private & Public Beta (ref. C2328).
c. **Annex 1 of Joint Schedule 11 (Processing Data**)
d. **Appendix 2 - Security Schedule** of this Order Form describes the Security requirements of the Authority.

6. Call-Off Deliverables

Call-Off Schedule 20 (Call-Off Specification) outlines the full requirements specification of services to be delivered. The Supplier's proposal is attached at Appendix 3.

7. 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 referred to in Framework Schedule 1 (Specification).

8. Cyber Essentials Scheme

The Buyer requires the Supplier, in accordance with Call-Off Schedule 26 (Cyber Essentials Scheme) to provide a Cyber Essentials Plus Certificate prior to commencing the provision of any Deliverables under this Call-Off Contract.

9. Maximum Liability

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms as amended by the Framework Award Form Special Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £813,950.00 Ex-VAT.

10. Call-Off Charges

Fixed Price: **REDACTED TEXT under FOIA Section 43, Commercial Interests**

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.

11. Reimbursable Expenses

None

12. Payment Method

The payment method is as detailed in Clause 4 of the Core Terms . All payments shall be made in accordance with Call-Off Schedule 5 (Pricing Details and Expenses Policy). The payment method for this Call-Off Contract is invoice and BACS.

13. Buyer's Invoice Address

Invoices will be sent to:
REDACTED TEXT under FOIA Section 40, Personal Information

All invoices should be sent, quoting a valid Cabinet Office purchase order number (PO Number), to: **REDACTED TEXT under FOIA Section 40, Personal Information**

We will send you a unique PO Number to **REDACTED TEXT under FOIA Section 40, Personal Information** once this agreement has been executed by both parties. You must be in receipt of a valid PO Number before submitting an invoice.

To avoid delay in payment it is important that the invoice is compliant and that it includes a valid PO Number, and the details (name and telephone number) of your customer contact (i.e. Contract Manager), and also what is being purchased. Non-compliant invoices will be sent back to you, which may lead to a delay in payment.

If you have a query regarding an outstanding payment, please contact **REDACTED TEXT under FOIA Section 40, Personal Information**

14. Buyer's Authorised Representative

REDACTED TEXT under FOIA Section 40, Personal Information

15. Buyer's Environmental Policy
Cabinet Office Environmental Policy Statement, 26 October 2017, Available online at
https://www.gov.uk/government/publications/cabinet-office-environmental-policy-statement

16. Supplier's Authorised Representative

REDACTED TEXT under FOIA Section 40, Personal Information

17. Supplier's Contract Manager
REDACTED TEXT under FOIA Section 40, Personal Information

18. Progress Report Frequency

Progress reports issued at each milestone or month, whichever is sooner.

19. Progress Meeting Frequency

Daily standups combined with a weekly progress meeting combined with problem solving session

To be held either virtual via Googlemeets (or equivalent) or shall be conducted at the Buyers Address. Framework Schedule 6 (Order Form, Statement of Work and Call-Off Schedules) OFFICIAL 7. Additional ad hoc meetings may be agreed between both parties as detailed in the Call-Off Schedule 20 (Specification).

20. Key Staff

REDACTED TEXT under FOIA Section 40, Personal Information

21. Key Subcontractor(s)

As per Joint Schedule 6 (Key Subcontractors).

22. Commercially Sensitive Information

REDACTED TEXT under FOIA Section 43, Commercial Interests

23. Balanced Scorecard

None

24. Material KPIs

Details can be found within Call-Off Schedule 20 (Specification) – Section 15 Service Levels and Performance.

25. Additional Insurances

As per Joint Schedule 3 (Insurance Requirements)

26. Guarantee

Not applicable

27. Social Value Commitment

Not applicable

28. 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:

Signature: **REDACTED TEXT under FOIA Section 40, Personal Information**

Name: **REDACTED TEXT under FOIA Section 40, Personal Information**

Cabinet Office

Role: **REDACTED TEXT under FOIA Section 40, Personal Information**

Date: 07 March 2023

For and on behalf of the Buyer:

Signature: **REDACTED TEXT under FOIA Section 40, Personal Information**

Name: **REDACTED TEXT under FOIA Section 40, Personal Information**

Role: **REDACTED TEXT under FOIA Section 40, Personal Information**

Date: 09/03/23

Appendix 1- The first Statement(s) of Works

The first Statement(s) of Works shall be inserted into this Appendix 1 as part of the executed Order Form. Thereafter, the Buyer and Supplier shall complete and execute Statement of Works (in the form of the template Statement of Work in Annex 1 to the template Order Form in Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules).

Each executed Statement of Work shall be inserted into this Appendix 1 in chronology.

Statement of Work

1 Statement of Works (SOW) Details

Upon execution, this SOW forms part of the Call-Off Contract (reference below).

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: 08.03.23

SOW Title: Statement of Work 01

Call-Off Contract Reference: C2328 Performance & Assurance Online Tooling Platform

Buyer: Cabinet Office

Supplier: Rainmaker Solutions

SOW Start Date: 08.03.23

SOW End Date: 24.01.23

Duration of SOW: 46 weeks

Key Personnel (Buyer): REDACTED TEXT under FOIA Section 40, Personal Information

Key Personnel (Supplier): REDACTED TEXT under FOIA Section 40, Personal Information

2 Call-Off Contract Specification – Deliverables Context

REDACTED TEXT under FOIA Section 43, Commercial Interests

3 Buyer Requirements – SOW Deliverables

REDACTED TEXT under FOIA Section 43, Commercial Interests

4 Charges

Call Off Contract Charges:

The applicable charging method(s) for this SOW is:

- Capped Time and Materials

The estimated maximum value of this SOW (irrespective of the selected charging method) is **REDACTED TEXT under FOIA Section 43, Commercial Interests**

REDACTED TEXT under FOIA Section 43, Commercial Interests

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 Order Form and incorporated into the Call-Off Contract and be legally binding on the Parties:

For and on behalf of the Supplier

Name: **REDACTED TEXT under FOIA Section 40, Personal Information**

Title: **REDACTED TEXT under FOIA Section 40, Personal Information**

Date: 07 March 2023

Signature: **REDACTED TEXT under FOIA Section 40, Personal Information**

For and on behalf of the Buyer

Name: **REDACTED TEXT under FOIA Section 40, Personal Information**

Title: **REDACTED TEXT under FOIA Section 40, Personal Information**

Date: 09/02/23

Signature: **REDACTED TEXT under FOIA Section 40, Personal Information**

Annex 1 (Template Statement of Work)

1 Statement of Works (SOW) Details

Upon execution, this SOW forms part of the Call-Off Contract (reference below).

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 – Deliverables 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 Type(s), for example Ad hoc, Inception, Calibration or Delivery]

3 Buyer Requirements – SOW Deliverables

Outcome Description:

Milestone	Milestone Description	Acceptance Criteria	Due Date	Payment

Ref				Tranche
MS01				
MS02				
MS03				
MS04				
MS05				
MS06				

Delay Payments:

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 Certificate][OR Cyber Essentials Plus Certificate]** for the work undertaken under this SOW, in accordance with Call-Off Schedule 26 (Cyber Essentials Scheme).

SOW Standards:

[**Insert** 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:

[**Insert** details of Material KPIs that have a material impact on Contract performance]

Material KPIs	**Target**	**Measured by**

[**Insert 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**	**Employment / Engagement Route (incl. inside/outside IR35)**

[**Indicate**: whether there is any requirement to issue a Status Determination Statement]

SOW Reporting Requirements:

[Further to the Supplier providing the management information detailed in Paragraph 6 of 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 does this requirement apply to?	Required regularity of Submission
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**].

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.]

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 Order Form and incorporated into the Call-Off Contract and be legally binding on the Parties:

For and on behalf of the Supplier

Name:

Title:

Date:

Signature:

For and on behalf of the Buyer

Name:

Title:

Date:

Signature:

Appendix 2: Security Schedule

1. Buyer Options

1.1. 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 Subcontractors 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:

2.1.1. comply with all requirements of this Schedule (*Security Management*); and
2.1.2. 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 Schedule (*Security Management*) except:

2.2.1. Paragraph 9 (*Security Management Plan*);
2.2.2. paragraph 9 of the Security Requirements (*Code Reviews*);
2.2.3. paragraph 11 of the Security Requirements (*Third-party Software Modules*);
2.2.4. paragraph 12 of the Security Requirements (*Hardware and software support*);
2.2.5. paragraph 13 of the Security Requirements (*Encryption*); and
2.2.6. 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 (*Security Management*):

"Anti-virus Software"	means software that: **(a)** protects the Supplier Information Management System from the possible introduction of Malicious Software; **(b)** scans for and identifies possible Malicious Software in the Supplier Information Management System; **(c)** if Malicious Software is detected in the Supplier Information Management System, so far as possible: **(i)** prevents the harmful effects of the Malicious Software; and **(ii)** 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:

	(a) 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; **(d)** 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 **(e)** any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements; **(f)** the installation of Malicious Software in the: **(i)** Supplier Information Management System; **(ii)** Development Environment; or **(iii)** Developed System; **(g)** any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the: **(i)** Supplier Information Management System; **(ii)** Development Environment; or **(iii)** Developed System; and **(h)** includes any attempt to undertake the activities listed in sub-paragraph (a) where the Supplier has reasonable grounds to suspect that attempt: **(i)** was part of a wider effort to access information and communications technology by or on behalf of Central Government Bodies; or **(ii)** was undertaken, or directed by, a state other than the United Kingdom

"Buyer Data"	means any: **(a)** 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; **(b)** Personal Data for which the Buyer is a, or the, Data Controller; or **(c)** any meta-data relating to categories of data referred to in paragraphs (a) or (b); that is: **(a)** supplied to the Supplier by or on behalf of the Buyer; or **(b)** 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: **(a)** has been certified by the National Cyber Security Centre; **(b)** holds "Green Light" status; and **(c)** 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: **(a)** the source code; **(b)** the object code; **(c)** third-party components, including third-party coding frameworks and libraries; and **(d)** all supporting documentation.
"Code Review"	means a periodic review of the Code by manual or automated means to: **(a)** identify and fix any bugs; and **(b)** ensure the Code complies with: **(i)** the requirements of this Schedule (*Security Management*); and **(ii)** 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: **3.1.1.** coding; **3.1.2.** testing; **3.1.3.** code storage; and **3.1.4.** 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-reference-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: **(a)** 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); **(b)** where that activity is performed by individuals, the place or facility from where that activity is performed; and **(c)** in respect of the entity providing the Support Locations or Third-Party Tools, its: **(i)** full legal name; **(ii)** trading name (if any) **(iii)** country of registration; **(iv)** registration number (if applicable); and **(v)** registered address.
"**Relevant Activities**"	means those activities specified in paragraph 0 of the Security Requirements.

"**Relevant Certifications**"	means **(a)** in the case of a standard agreement: **(i)** Cyber Essentials; and/or **(ii)** Cyber Essentials Plus as determined by the Buyer; or **(b)** in the case of a higher risk agreement: **(i)** 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 **(ii)** 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: **(a)** 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 **(b)** 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:

	(a) they will not contract other than on their own contractual terms; and **(b)** either: **(i)** there are no other substitutable suppliers of the particular services other than SMP Sub-contractors; or **(ii)** the Sub-contractor concerned has an effective monopoly on the provision of the Services.
"**Sites**"	means any premises: **(a)** from or at which: **(i)** the Services are (or are to be) provided; or **(ii)** the Supplier manages, organises or otherwise directs the provision or the use of the Services; or **(b)** where: **(i)** any part of the Supplier Information Management System is situated; or **(ii)** any physical interface with the Buyer System takes place; and **(c)** for the avoidance of doubt include any premises at which Development Activities take place
"**Sub-contractor**"	includes, for the purposes of this Schedule (*Security Management*), any individual or entity that: **(a)** forms part of the supply chain of the Supplier; and **(b)** 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: **(a)** any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and **(b)** engaged in or likely to be engaged in: **(i)** the performance or management of the Services;

	(ii) or the provision of facilities or services that are necessary for the provision of the Services.
"**Supplier Information Management System**"	means: **(a)** 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; **(b)** the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources); and **(c)** for the avoidance of doubt includes the Development Environment.
"**Security Requirements**"	mean the security requirements in Annex 1 to this Schedule (*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: **(a)** is not produced by the Supplier or a Sub-contractor as part of the Development Activity; and **(b)** either: **(i)** forms, or will form, part of the Code; or **(ii)** 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 Schedule (*Security Management*) sets out:

4.1.1. the assessment of this Agreement as either a:

higher risk agreement; or

standard agreement,

in Paragraph 1;

4.1.2. 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:

the Development Activity;

the Development Environment;

the Buyer Data;

the Services; and

the Supplier Information Management System;

4.1.3. the principle of co-operation between the Supplier and the Buyer on security matters, in Paragraph 5;

4.1.4. the Buyer's access to the Supplier Personnel and Supplier Information Management System, in Paragraph 7;

4.1.5. the Certification Requirements, in Paragraph 8;

4.1.6. the requirements for a Security Management Plan in the case of higher-risk agreements, in Paragraph 9; and

4.1.7. 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:

the Sites;

the Services; and

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:

5.3.1. 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;

5.3.2. the security and integrity of the Developed System; and

5.3.3. 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:

6.1.1. comply with the Security Requirements; and

6.1.2. 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:

6.2.1. use best endeavours to ensure that the SMP Sub-contractor complies with the Security Requirements;

6.2.2. 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;

6.2.3. 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:

7.1.1. access to the Supplier Personnel, including, for the avoidance of doubt, the Sub-contractor Personnel;

7.1.2. 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

7.1.3. 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 Schedule (*Security Management*) and the Security Requirements.

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

7.2.1. in the case of a Breach of Security within 24 hours of such a request; and

7.2.2. 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:

8.1.1. it; and

8.1.2. 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:

8.2.1. the Relevant Certifications for it and any Sub-contractor; and

8.2.2. 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:

8.3.1. currently in effect;

8.3.2. cover at least the full scope of the Supplier Information Management System; and

8.3.3. 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:

8.4.1. a Relevant Certification has been revoked or cancelled by the body that awarded it;

8.4.2. a Relevant Certification expired and has not been renewed by the Supplier;

8.4.3. a Relevant Certification no longer applies to the full scope of the Supplier Information Management System; or

8.4.4. 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:

8.5.1. 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:

8.5.1.1. full details of the Certification Default, including a root cause analysis;

8.5.1.2. the actual and anticipated effects of the Certification Default;

8.5.1.3. the steps the Supplier and any Sub-contractor to which the Certification Default relates will take to remedy the Certification Default;

8.5.2. the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;

8.5.3. 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;

8.5.4. the rejection by the Buyer of a revised Certification Rectification Plan is a material Default of this Agreement;

8.5.5. 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 Schedule (*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:

9.3.1. an assessment of the Supplier Information Management System against the requirements of this Schedule (*Security Management*), including the Security Requirements;

9.3.2. 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

9.3.3. the following information, so far as is applicable, in respect of each Sub-contractor:

9.3.3.1. the Sub-contractor's:

9.3.3.1.1. legal name;

9.3.3.1.2. trading name (if any);

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

9.3.3.2. the Relevant Certifications held by the Sub-contractor;

9.3.3.3. the Sites used by the Sub-contractor;

9.3.3.4. the Development Activity undertaken by the Sub-contractor;

9.3.3.5. the access the Sub-contractor has to the Development Environment;

9.3.3.6. the Buyer Data Processed by the Sub-contractor;

9.3.3.7. the Processing that the Sub-contractor will undertake in respect of the Buyer Data;

9.3.4. the measures the Sub-contractor has in place to comply with the requirements of this Schedule (*Security Management*);

9.3.5. the Register of Support Locations and Third Party Tools;

9.3.6. the Modules Register;

9.3.7. the Support Register;

9.3.8. details of the steps taken to comply with:

9.3.8.1. the Secure Development Guidance; and

9.3.8.2. the secure development policy required by the ISO/IEC 27001:2013 Relevant Certifications;

9.3.9. details of the protective monitoring that the Supplier will undertake in accordance with paragraph 20 of the Security Requirements, including:

9.3.9.1. the additional audit and monitoring the Supplier will undertake of the Supplier Information Management System and the Development environment; and

9.3.9.2. 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:

9.4.1. an information security approval statement, which shall confirm that the Supplier may use the Supplier Information Management System to:

9.4.1.1. undertake the Development Activity; and/or

9.4.1.2. Process Buyer Data; or

9.4.2. 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:

9.8.1. a significant change to the components or architecture of the Supplier Information Management System;

9.8.2. a new risk to the components or architecture of the Supplier Information Management System;

9.8.3. a vulnerability to the components or architecture of the Supplier Information Management System using an industry standard vulnerability scoring mechanism;

9.8.4. a change in the threat profile;

9.8.5. a significant change to any risk component;

9.8.6. a significant change in the quantity of Personal Data held within the Service;

9.8.7. a proposal to change any of the Sites from which any part of the Services are provided; and/or

9.8.8. 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 SC 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 Schedule ◆(*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 contract 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 Schedule ◆(*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 Suppler 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.

Provider "Security Management Plan required for inclusion.

Appendix 3: Proposal

REDACTED TEXT under FOIA Section 43, Commercial Interests